ASIGNACIÓN INDEBIDA DE COMPETENCIA A LOS JUECES PENALES MUNICIPALES FRENTE A LOS DELITOS INFORMATICOS

DIANA CAROLINA COTRINA VIDAL

CRISTIAN MANUEL PUENTES MORA

UNIVERSIDAD MILITAR NUEVA GRANADA

FACULTAD DE DERECHO

BOGOTÁ D.C 2018

ASIGNACIÓN INDEBIDA DE COMPETENCIA A LOS JUECES PENALES MUNICIPALES FRENTE A LOS DELITOS INFORMATICOS

DIANA CAROLINA COTRINA VIDAL

CRISTIAN MANUEL PUENTES MORA

MONOGRAFÍA PARA OBTENER EL TITULO DE

ABOGADO

ASESOR: DOCTOR MAURICIO HENAO BOHORQUEZ

ABOGADO

UNIVERSIDAD MILITAR NUEVA GRANADA

FACULTAD DE DERECHO

BOGOTÁ D.C

2018

UNIVERSIDAD MILITAR NUEVA GRANADA

FACULTAD DE DERECHO

HOJA DE APROBACIÓN DE MONOGRAFIA

ASIGNACIÓN INDEBIDA DE COMPETENCIA A LOS JUECES PENALES MUNICIPALES FRENTE A LOS DELITOS INFORMATICOS

Monografía aprobada por:

Director: Doctor Mauricio Henao Bohórquez

Fecha:

Esta monografía de grado la queremos dedicar en primer lugar a la Academia. A nuestras familias, María Carolina Mora, Jackeline del Socorro Vidal, Mercedes Valbuena Vda de Puentes y José Manuel Puentes Valbuena, por sus consejos, su dedicación y su apoyo. A la universidad Militar Nueva Granada por su excelente labor académica y formación profesional recibida, a nuestro Abogado asesor por su inigualable guía académica, humana, metodología y por su apoyo incondicional para el desarrollo de nuestro tema de estudio a desarrollar.

A nuestra Alma Mater, Universidad Militar Nueva Granada.

Damos nuestra más sincera muestra de gratitud al Doctor Mauricio Henao Bohórquez, por su entera dedicación, apoyo y todos los aportes académicos para el desarrollo de nuestras ideas que hoy se encuentran plasmadas en esta monografía de grado.

RESUMEN

El derecho a lo largo de la historia se ha adaptado a los cambios presentes en la sociedad, actualizándose de manera constante y generando nuevas normas que permitan regular la conducta de los miembros de la sociedad, conforme esta última avanza.

Por esta razón, el surgimiento de las novedosas herramientas tecnológicas e informativas, implicó un reto para los legisladores a nivel mundial, lo anterior por las nuevas relaciones jurídicas que represento la aparición de estas nuevas tecnologías. Encontrándose dentro de estas relaciones, aquellas que vulneraban el ordenamiento jurídico en el ámbito penal, razón por la que en diferentes países se empezó a acuñar el término de "delitos informáticos".

Esta nueva noción implico para el mundo jurídico, la necesidad de generar una normatividad sustancial y procesal en la materia. Para el caso colombiano se profirió la ley 1273 de 2009, norma que adiciona a la ley 599 del 2000 el título VII BIS de la protección de la información y de los datos, con 10 artículos que buscan castigar las conductas punibles que atenten contra estos nuevos bienes jurídicamente tutelados, siendo una de las normas más severas a nivel mundial, sus sanciones no solo son económicas, también privativas de la libertad.

Sin embargo, en materia procesal no se generó un cambio estructural en materia de competencia para los jueces penales que deben dirimir los conflictos en los que se encuentren involucrados delitos informáticos. Por este motivo la presente investigación,

pretende analizar la idoneidad de los jueces penales municipales para juzgar los delitos informáticos, en punto de la competencia funcional que debe tener el juzgador.

Palabras clave: Derecho informático, delitos informáticos, TIC, competencia, protección de datos, cibercrimen, ciberdelincuentes, seguridad informática.

ABSTRACT

The right throughout history has been adapted to the changes present in society, constantly updated and generating new rules that allow regulating the behavior of members of society, as the latter progresses.

For this reason, the emergence of new information technologies, implied a challenge for legislators worldwide, the above by the new legal relationships that represent the emergence of these new technologies. Being within these relationships, those that violated the legal system in the criminal field, which is why in different countries the term "computer crimes" began to be coined.

This new notion implied for the legal world, the need to generate a substantial and procedural normativity in the matter. For the Colombian case, Law 1273 of 2009 was issued, a rule that adds to the law 599 of 2000 the title VII BIS of the protection of information and data, with 10 articles that seek to punish the punishable conducts that attempt against these new ones legally protected, being one of the most severe rules worldwide, its sanctions are not only economic, also depriving of freedom.

However, procedural matters did not generate a structural change in competition for criminal judges who must settle disputes in which computer crimes are involved. For this reason, the present investigation intends to analyze the suitability of municipal criminal judges to judge computer crimes, in terms of the functional competence that the judge should have.

Keywords: Computer law, computer crimes, ICT, competition, data protection, cybercrime, cybercriminals, computer security.

CONTENIDO

INTRODUCCIÓN

Los avances tecnológicos del último siglo han participado en el desarrollo económico, social, cultural y educativo en todo el mundo, de tal modo que las personas son dependientes de sus dispositivos tecnológicos y la conexión permanente a internet, no solamente para espacios de ocio, también en el ejercicio profesional, influyendo en la celebración de contratos, negocios, transacciones bancarias y todo tipo de cargas laborales en donde se interactúa constantemente y prácticamente a tiempo real con cualquier individuo a nivel mundial, utilizando la tecnología en casi un 65% de sus acciones cotidianas, aumentando a diario con la el avance tecnológico al punto de la necesidad domótica y el internet de las cosas. Debido a este avance tecnológico la presencia física de las personas se vuelve prácticamente innecesaria, reduciendo los ataques de los delincuentes de manera física, dicha circunstancia invita al delincuente a introducirse en el campo de la tecnología para crear nuevos métodos delictivos, afectando de igual manera el patrimonio de las personas e inclusive su vida personal.

La finalidad de este trabajo de investigación se enmarca en identificar el nivel idoneidad de los juzgadores de este tipo de delitos, con el fin de poder identificar la consecuente eficacia de su actuar y en consecuencia proponer alternativas frente a esto.

En la actualidad la mayoría de nuestra información se encuentra en la Internet, por esta razón se necesitan medidas que protejan eficazmente la información de todas las personas, permitiendo la correcta manifestación de la justicia por medio del ejercicio penal cuando así sea pertinente.

Los precedentes judiciales en la actualidad, evidencian la falta de conocimiento de los jueces penales municipales respecto a delitos informáticos, unos por falta de conocimiento y otros por mala interpretación de los hechos punibles cometidos a través de medios informáticos.

Absolver delitos que pueden llegar a tener una afectación patrimonial bastante cuantiosa, condenar personas por desconocimiento del funcionamiento de algunos dispositivos tecnológicos, son algunos de los errores cometidos dada la incompetencia de aquellos que emitieron juicio, en intención cualquiera, pero en incapacidad para cumplir con el ordenamiento jurídico.

Como consecuencia de lo anterior, en el presente trabajo se proyectó como objetivo general Identificar la idoneidad de los jueces penales municipales en la aplicación de los delitos informáticos, teniendo en cuenta la eficacia de sus decisiones con respecto a la solución de conflictos en lo que se estudien delitos informáticos, en relación con la competencia asignada legalmente.

Por tal razón siguiendo los lineamientos establecidos dentro del objetivo general, proyectaron los siguientes objetivos específicos:

1. Identificar el estado de los delitos informáticos en Colombia, desde una perspectiva doctrinal y legislativa.
2. Analizar la jurisprudencia colombiana foránea, referente a los delitos informáticos.
3. Proponer un sistema de competencia que optimice la idoneidad de los jueces penales.

Por otro lado, el Método de investigación que será usado es de carácter cualitativo, se realizará análisis respectivo del ordenamiento jurídico procesal nacional estableciendo las principales problemáticas que traen consigo la indebida asignación de competencia a los jueces penales municipales, analizando las fuentes jurídicas nacionales, sentencias emitidas por autoridades nacionales e internacionales, con fuentes estadísticas y pronunciamientos de las autoridades internacionales en la materia específica.

Por lo anterior, y teniendo en cuenta los objetivos de investigación y el trayecto a desarrollar dentro de la presente investigación se pretende establecer ¿Cuál es el nivel de idoneidad de los jueces penales municipales para conocer de delitos informáticos?

CAPÍTULO I. ASPECTOS GENERALES

Es importante fijar los aspectos básicos a desarrollar dentro del presente trabajo investigativo, toda vez, que mediante la contextualización de los temas elementales que deben ser abordados dentro de la delincuencia informática, se entenderá zde una manera más sencilla la importancia mundial que junto con los avances tecnológicos ha tenido esta temática, y de esta manera, poder demostrar y determinar la afectación que ha generado la ciberdelincuencia en diversos aspectos y campos a nivel mundial; cerrando de ésta manera el presente trabajo, con el estudio de las pocas medidas fijadas para el tratamiento de esta problemática en nuestro país, y adicional a esto, plantear un análisis que aborde la necesidad de plantear una actualización a la normatividad vigente, con la finalidad de que ésta sea acorde a los avances que se presentan constantemente en nuestra sociedad. Por lo anterior abordaremos nuestra temática de investigación de la siguiente manera:

1. Definición Derecho Informático

Como introducción a los temas que abordaremos en el presente capítulo, encontramos que de Conformidad con lo expuesto por Carlos A. Peña se denomina Derecho informático:
A la universalidad de problemas que surgen de las transformaciones que el derecho ha ido realizando como imposición de ciertas actividades novedosas que se desarrollan en el ámbito social y que requieren nuevas regulaciones o una interpretación de las regulaciones ya existentes a fin de dar respuestas en el sentido de la justicia (Peña).

De esta manera, vemos como esta definición, nos demuestra la existencia de una problemática que avanza a pasos agigantados a nivel global, y hace un llamado, a la actualización y la implementación de diversas medidas que permitan una regulación cada día más eficaz de ésta problemática, que tiene un avance notablemente rápido en nuestro entorno social.

Por ende podemos definir como complemento al concepto citado, al Derecho informático, como ésta rama del Derecho, que regula los temas informáticos que pruducen un efecto jurídico dentro de nuestra sociedad, regulando de esta manera no solamente cuestiones de delincuencia informática, sino también una diversidad de temásticas jurídicas que han evolucionado a través del tiempo y que hoy en día también cuentan con una regulación normativa dentro del ámbito informático.

1.1. Delitos Informáticos

En concordancia con lo expuesto anteriormente, dentro del presente título es importante señalar que, el Derecho es una profesión que debe evolucionar de manera constante, como evoluciona nuestra sociedad, y es así como nos damos cuenta, que éste avance social se desarrolla de una manera rápida el tiempo, razón por la cual, nuestra profesión nos exige implementar diariamente en nuestro desempeño como abogados, la ejecución de mecanismos y hábitos que nos permitan permanecer en equilibrio con los avances sociales y jurídicos que se desarrollan periódicamente.

Observamos de esta manera, que de conformidad con la aparición de las diversas problemáticas de orden social, el derecho se ve en la obligación de establecer normativas que concluyan en una regulación jurídica de estas conductas y de este modo, mantener en gran parte un equilibrio social, que nunca será completo.

Por ende, actualmente, vemos que las nuevas tecnologías se convirtieron en mecanismos que facilitan la realización de las tareas diarias que desempeñamos los individuos a lo largo del mundo, y que de cierta forma facilitan nuestra vida y nos permiten una optimización de nuestro desempeño en los diversos aspectos de nuestra existencia.

Por tal razón, estas herramientas electrónicas, a la vez, crean un portal, en el que se entra desarrollar el tema de la delincuencia informática, toda vez, que de la misma manera en que facilitan nuestro diario vivir, también se convierten en elementos, desde los cuales, los ciberdelincuentes de una manera más sencilla y rápida, pueden llegar a cometer una

diversidad de delitos informáticos, que afectan tanto a personas jurídicas y naturales, y que además de esto por el anonimato y la protección de identidad que en cierto punto permite Internet, hace que la labor de rastreo que se hace a estos individuos en muchos casos sea complicada, y es por tal motivo que se requiere la vinculación de personal con conocimientos en esta temática operacional, y de una actualización constante de la normatividad aplicable que avance junto con la aparición de las diversas conductas delictivas que se ejecutan de manera cibernética.

1.2. Definición

Se entiende por Delito todo acto que constituya un quebrantamiento de la ley y en cuanto a informático aquel conjunto de métodos y técnicas que posibilitan y facilitan el manejo de la información. Dado esto, a pesar de que los interesados en el tema no encuentran terreno común al respecto, y en virtud de esta investigación se definirá "Delito Informático" como todo quebrantamiento de la ley en el que se haga participe algún conocimiento o técnica que haga posible el tratamiento automático de la información.

En cuanto a los delitos informáticos no podemos encontrar una definición estándar o establecida, su condición abarca una gran cantidad de conductas de las que se pueden desprender distintos significados para hacer referencia a las conductas delictivas que se cometen a través de medios informáticos e internet.

2. Clasificación de los delitos informáticos

En relación al tema objeto de estudio, se puede determinar y resaltar, que las principales conductas relacionadas con la delincuencia informática, ejecutadas no solo a nivel nacional sino también internacional son las siguientes:

Delitos relacionados con propiedad intelectual	Dentro de este grupo se destaca la vulneración a los derechos de autor, programas informáticos, y alteración de bases de datos.
Delitos relacionados con el Derechos a la intimidad personal.	En este espacio se precisa, que este tipo de vulneración se produce por la publicaicón, acopio, alteración entre otras conductas de los datos personales de los individuos afectados
Delitos que afectan el patrimonio, o genera una afectación principalmente económica a sus víctimas.	En este punto se desarrollan aquellos delitos que atentan contra el patrimonio de los afectados, principalmente por la sustracción de información, propagación de virus, espionaje entre otros.

Sin embargo, es importante resaltar que como lo expresa el autor Jacobo Gamba:

Se ha visto que la estrategia de modificación normativa no es suficiente, y en algunos casos, como en la Unión Europea, se empezaron a implementar algunas medidas no legislativas. Entre ellas cabe recordar la creación de unidades nacionales especializadas (autoridades policiales y autoridades judiciales); la formación permanente y especializada de policías y personal de la administración de justicia; la armonización de las normas de contabilización en materia policial y judicial así como la creación de instrumentos adaptados para el análisis estadístico de la criminalidad informática; creación de acciones realizadas directamente por las empresas con el fin de luchar contra la delincuencia informática; implementación de proyectos en el ámbito de la investigación y el desarrollo tecnológico (Jacopo, 2010).

3. Características de Delitos Informáticos.

De conformidad con lo expuesto por el abogado e investigador mexicano sobre delincuencia informática Julio Téllez Valdés, los delitos informáticos poseen las siguientes características,

a) Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.
b) Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se haya trabajado.

c) Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
d) Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios económicos "al hechor."
e) Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
f) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
g) Son muy sofisticados y relativamente frecuentes en el ámbito militar.
h) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
i) En su mayoría son imprudenciales y no necesariamente se cometen con intención (Valdes, 1991).

4. Antecedentes Históricos

Recordamos que el desarrollo y la evolución de los delitos informáticos se genera conjuntamente con la evolución de las herramientas tecnológicas alrededor del mundo; es por tal razón que con el avance de estos medios tecnológicos, también se ha generado un avance en la manera en la que se efectúa la comisión de conductas delictivas, que han encontrado gran provecho y beneficio en la implementación de los medios electrónicos para la comisión de diversos delitos informáticos, cuyos avances, y aparición de nuevas conductas punibles, se generan periódica y habitualmente.

Podrá parecer a quienes conozcan de derecho informático, extraño, pero la primera aplicación de dichas herramientas se dio con la intercepción de información, fue en tiempo de guerra y no correspondió en su momento con quebrantamiento de la ley, compete para esta investigación reconocer este hecho más no emitir juicio moral al respecto.

La introducción de los ordenadores en determinados ámbitos sociales tuvo lugar por la década de los años 50 construida la primera computadora digital la ENIAC (Electronic Numerical and Computer) diseñada y construida por los ingenieros John Presper Eckert y John William Maucly, que por aquella época se le denominaba computadora, pues era la traducción directa y textual del inglés "computer" que, no obstante, se sigue utilizando en el derecho comparado (Guerra). Ha habido algunos intentos en nuestra doctrina de cambios de terminología, e incluso de modificar el término actual de ordenador, como por ejemplo por el de elaborador electrónico (Bolaño & Tarriba , 2012).

Para el año de 1949, Norver Wiener, publicó una obra en cuyo capítulo IV, denominado el "Derecho y las Comunicaciones" el cual expresa la influencia que ejerce la cibernética respecto a uno de los fenómenos sociales más significativos: El Jurídico (Norbert, 1980)

Adicional a esto Wiener manifiesta que el juez estadounidense Lee Loevinger publicó para ese mismo año de 1949, un artículo de 38 hojas en la revista Minesota Law Review, titulado "the Next step Forward" en donde menciona que el próximo paso en el largo camino del progreso del hombre, debe ser el de la transición de la Teoría general del

Derecho Hacia la Jurimetría, que es la investigación científica, acerca de los problemas jurídicos (Norbert, 1980).

Los primeros estudios empíricos del delito informático o delito vinculado a la informática se llevaron a cabo a partir de mediados de los años 70, aplicando métodos científicos de investigación criminológica (División de Investigación y Desarrollo del Consejo Nacional de la Prevención del Delito, 1981), identificándose el primer caso de delito informático en dicho informe, el caso de Draper Jhon, en septiembre de 1970 (Bolaño & Tarriba , 2012).

Finalmente es relevante mencionar que uno de los primeros y más importantes ataques en la historia de Internet se remonta a CREEPER en 1971, escrito por el ingeniero Bob Thomas, y es considerado el primer virus informático que afecto a una computadora el cual mostraba un mensaje en los equipos infectados, el cual, si no causaba daño alguno, fue la base para el desarrollo de ataques posteriores con pérdidas multimillonarias (González, 2013).

4.1 Referencias internacionales sobre los delitos informáticos

4.1.1. España

El continente Europeo es quizá uno de los más importantes en materia tecnológica y regulación de la misma, el avance tecnológico a obligado al poder legislativo Europeo a regular estas nuevas condiciones tecnológicas que influyen en sus nacionales, se puede decir que España es quizá el país que tiene la mejor regulación jurídica en cuanto a delitos informáticos , se puede decir que el avance tecnológico ha tenido un punto de acceso

importante y en el que se ha obligado al avance legislativo para salvaguardar los derechos de sus nacionales, de este avance tecnológico encontramos con la mayor fortaleza jurídica a España quien a establecido quizá una de las legislaciones más fuertes y mejores estructuradas frente al tema de delitos informáticos.

España ha sido considerado el país con más experiencia en el manejo de delitos informáticos en toda Europa, organizada por una ley penal orgánica (Ley 10 /1995 de 23 de noviembre), la cual fue reformada por la (ley 1/2015 30 de Marzo), esta ley establece las conductas típicas de carácter informático, las modalidades y su respectiva sanción penal.

De conformidad con el Doctor Santiago Acurio del Pino:

El presente Código Penal incorporó a los tipos delictivos clásicos la realidad informática de manera global, no limitándose a regular solo los delitos informáticos de mayor conocimiento en la doctrina y otras legislaciones. Es inobjetable su intento por lograr la armonía jurídica entre las figuras clásicas penales y el fenómeno informático, lo cual requiere de un gran esfuerzo, no tanto así la solución que han adoptado otros ordenamientos jurídicos, los cuales se han limitado a enfrentar el problema a través de leyes especiales, que consideran al fenómeno informático aislado del resto de la legislación, apartándose de la buena técnica jurídica, como en el caso de Chile (Pino, 2008).

Incluyendo estas conductas delictivas dentro de los delitos económicos de acuerdo a el tipo de afectación y por su naturaleza patrimonial, siendo aquellas dirigidas a cualquier tipo de fraude informático que se encuentre relacionado con la extracción de información financiera, estos delitos se encaminan en relación del acceso no autorizado en sistemas

informáticos en los cuales se busca defraudar al sistema informático que contiene la información sensible realizando modificaciones de las mismas para hacer transferencias bancarias no autorizadas.

Otros delitos que buscan ser castigados son, las calumnias e injurias que se difunden en cualquier medio de comunicación, los fraudes y sabotajes informáticos, y la inducción a los menores a la prostitución, como también la realización y distribución de material pornográfico.

La denuncia del delito, se establece que, para proceder judicialmente frente a estos delitos, es necesario la denuncia de aquel que resulte afectado por la comisión de este delito o de su representante legal, de ser esta un menor de edad, o discapacitada, en estos casos puede proceder el Ministerio Fiscal.

Cabe resaltar que en España se encuentra la Unidad de Investigación Tecnológica, esta unidad se especializa en la investigación y seguimiento de las conductas relacionadas con delincuencia informática, con el fin de dar una protección al ciudadano en materia de protección al patrimonio, la protección a la propiedad industrial e intelectual, protección al menor, combatir la pornografía infantil, y todos aquellos delitos relacionados con las redes sociales.

Entre otras legislaciones que enmarcan los delitos informáticos, encontramos el Convenio sobre la Ciberdelincuencia – 23 de noviembre de 2011 – Consejo de Europa, este convenio

busca conseguir una unión entre sus miembros con el fin de combatir y cooperar entre ellos cuando de delitos informáticos se trate, en su preámbulo contempla lo siguiente:

Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional; Conscientes de los profundos cambios provocados por la digitalización, la convergencia y la globalización continua de las redes informáticas; Preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes (Convenio sobre la Ciberdelincuencia Budapest, 23.XI.2001).

Es notable la acción de los Estados miembros, en la prevención de la ciberdelincuencia y todas aquellas acciones en las cuales se atente los derechos de las personas, en cualquiera de las acciones tipificadas, es de esta forma como se busca proteger los sistemas informáticos por medio de este convenio, de forma rápida y efectiva para que la delincuencia relacionada con los delitos informáticos en su mayor parte sea reducida o exterminada y brindar una mayor seguridad cuando de información se trate.

Las nociones del Convenio estarán encaminadas en la preservación de forma adecuada de los sistemas informáticos y todo lo que con ello acarrea como la preservación de la información y los delitos en los cuales una persona estaría en curso, cada parte deberá

aportar medidas legislativas y tener en cuenta la jurisdicción y competencia cuando se deba conocer de un delito informático.

La Resolución del Concejo N. 2002 / C43, 28 de enero de 2002, es otra de la normativa en relación:

A un enfoque común y acciones específicas en materia de seguridad de las redes y de información, teniendo por objeto lo siguiente: asegurar la disponibilidad de servicios y datos, prevenir la interrupción e interceptación no autorizada de comunicaciones, dar confirmación de que los datos enviados, recibidos o almacenados son completos y no han sufrido modificaciones, garantizar la confidencialidad de los datos, proteger los sistemas de información de los accesos no autorizados, proteger de ataques efectuados mediante programas nocivos, garantizar una autenticación fiable (Resolución del Consejo No 2002/ C43, 2002).

Esta Legislación (Resolución del Consejo No 2002/ C43, 2002), toma en cuenta que el uso de los sistemas informáticos va creciendo cada vez con más fuerza, es obligación prestar una seguridad e ir creciendo conforme lo va haciendo la tecnología, para adecuar de mejor forma el uso de las mismas, esta legislación toma en cuenta temas como las transacciones económicas y el comercio electrónico, entre otros servicios en línea que son prestados, se debe tener la obligación de prestar una seguridad al usuario de estas plataformas. El uso de estos medios que han servido en gran medida a facilitar nuestras vidas, debe ser monitoreado y controlados con el fin de evitar un fraude electrónico para que la economía de quien es beneficiario de estos sistemas no se vea gravemente afectada.

También pone en consideración, que las disposiciones del poder público deben ser aún más poderosas y fuertes en el mundo europeo, para facilitar un mayor desempeño en los mercados internos y que estos mismos deben fundarse en la cooperación entre los Estados miembros para apoyar la innovación.

Es por esto, que se pide a los estados miembros lo siguiente, establecido en la Resolución del Consejo N° 2002/C 43, 28 enero 2002, que deben propagar información y educación para crear una sensibilización sobre el uso adecuado de la redes de la información, como el uso correcto de bases de datos entre otros y es deber de los Estados miembros poner en practica esta conciencia de seguridad informática, también en lo establecido por esta resolución y que busca un sistema de autenticación más seguro es el uso de la firma electrónica ya que es un mecanismo que prestara mayor seguridad y confianza.

Otra de la legislación que se relaciona con los delitos informáticos es la Propuesta de Decisión Marco del Consejo N° 2002/C 203, 19 abril 2002. "Relativa a los ataques de los que son objeto los sistemas de información", esta legislación explica los riesgos a los cuales corren los sistemas de información y las acciones que los Estados miembros deben realizar para combatir estas acciones delictivas.

Los tipos de irrupciones a los sistemas informáticos son una amenaza, que ataca las diferentes vías que los conectan, en esta propuesta se ha descrito los siguientes como las intimidaciones que se presentan hacia los sistemas informáticos, el acceso no autorizado a los sistemas de información, donde también se incluye la piratería informática, este tipo de ataque hace referencia en tener acceso de manera no autorizada a un computador o red de

computadores, con la ánimo te interceptar algo y con intención de destruir modificar o copiar datos.

Otro de los ataques a los que están vulnerables los sistemas, es la perturbación de los sistemas de información, que es la acción por la cual se busca deteriorar los servicios ofrecidos por internet, estos ataques son definidos por la propuesta de Decisión – Marco del Consejo como:

Uno de los medios más conocidos de denegar o deteriorar los servicios ofrecidos por Internet es el ataque de tipo "denegación de servicio" (DdS). Este ataque es en cierta medida similar al hecho de inundar las máquinas de fax con mensajes largos y repetidos. Los ataques del tipo denegación de servicio tienen por objeto sobrecargar los servidores o los proveedores de servicios Internet (PSI) con mensajes generados automáticamente. Otros tipos de ataques pueden consistir en perturbar los servidores que hacen funcionar el sistema de nombres de dominio (DNS) y los ataques contra los "encaminadores". Los ataques destinados a perturbar los sistemas han sido perjudiciales para algunos sitios web prestigiosos como los portales (Resolución del Consejo No 2002/ C43, 2002).

La ejecución de los programas nocivos que alteran o destruyen datos, son otro de los ataques a los sistemas de información, los virus o malware son una de los molestias más peligrosas, ya que la mayoría de las personas a sido a afectado al menos con uno de estos, estos programas maliciosos buscan dañar la información infectando de virus al computador y su acción es destruir o modificar datos, entre los más conocidos están, los virus “ I Love You”, “ Melisa” , “Kournikova” las llamadas “ bombas lógicas “, “caballos de Troya” y los llamados “Gusanos”.

La denominada “Sniffing” Interceptación de las comunicaciones, como hemos visto alrededor de la investigación afecta la confidencialidad de los datos informáticos, y otra de las acciones que atenta contra los sistemas son las declaraciones falsas conocidas como “Spoofing”, en cual su acción es suplantar una persona en la web con intención de causar algún tipo de daño, así lo define la descripción de la Propuesta de Decisión Marco del Consejo N° 2002/C 203, 19 abril 2002.

El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest, es otra de las fuentes investigativas por la cual se evidencia, la problemática de los delitos informáticos frente a la gran evolución que a tenido el uso de la Internet que puede llegar a la delincuencia, el autor Andrés Díaz Gómez considera lo siguiente frente a esta problemática: La red también es plataforma de terroristas de todo el mundo. Captar fondos o reclutar adeptos, hacer apología de sus ideas, planificar atentados, sembrar el terror psicológico o incluso atacar mediante hackers la infraestructura de un Estado, son posibilidades nada alejadas la realidad en que vivimos (Gomez, 2011).

El valor de los datos que se encuentran alojados por los servidores distribuidos por todo el globo, son indiscutiblemente preponderantes, esta información es almacenada en un centro de datos y el ataque a cualquiera de estas bases de información puede ser caótica, es de esta forma que nos enfrentamos al problema más importante ya que nos podemos llegar a preguntar ¿Y qué pasa con la información? Si es atacada o vulnerada para ser modificada, borrada, alterada y demás acciones delincuenciales.

En consecuencia, de este problema, el autor nos plantea lo siguiente:

Pero, además, y dado que a la Red se puede acceder desde cualquier parte del mundo prácticamente al instante, el siguiente problema relacionado con la independencia geográfica de Internet lo encontramos en la dificultad de perseguir un ilícito de estas características. Quiérase decir que un sujeto puede cometer un delito contra otro situado a miles de kilómetros del primero, mientas que la información está en otro lugar diferente de éstos. La situación puede llegar a producir una verdadera impunidad, si no se articulan los remedios adecuados (Gomez, 2011).

Las acciones delincuenciales, como lo explica el autor, se pueden generar con mucha facilidad y pueden venir de una persona quien no tenga muchos conocimientos informáticos, las acciones pueden ser, desde crear un virus o sabotear un programa informático, en consecuencia de esto la aplicabilidad de la Ley Penal refiere que estos delitos se pueden realizar desde cualquier lugar del mundo con la dificultad de saber en dónde se cometió, esto puede generar un problema con las jurisdicciones ya que se puede generar una laguna normativa en relación con la jurisdicción, el autor contempla lo siguiente en relación con este problema:

Es importante resaltar que muchas veces es difícil determinar cuál es la legislación nacional que se estaría violando, de existir alguna, ya que todo el contenido de Internet aparece simultáneamente en todo el mundo. Dentro de este contexto, prácticamente todas las actividades en Internet tienen un aspecto internacional que podría involucrar múltiples jurisdicciones o provocar el llamado efecto indirecto (Gomez, 2011).

Las acciones de Cibercriminalidad avanzan cada vez más conforme avanza el uso de las nuevas tecnologías, la cooperación de las entidades internacionales debe ser la clave para combatir estas acciones criminales, aunque no es fácil ya que hay que estar en constante movimiento de acuerdo a los avances y modificaciones del uso de estas tecnologías, como también la coordinación de las normas procesales que podrán hacer posible que el sistema jurídico funcione de una forma más ágil y que no se vuelvan en procesos largos y arduos. Los tratados internacionales también están en la obligación de velar en lo que concierne con los Derechos Humanos como se había tratado anteriormente.

La asignación de la competencia, en relación con los delitos informáticos debe tratarse de manera muy especial por diferentes razones, la primera de ella y la más importante debe ser el dónde se realizó, el origen del delito ya que se puede cometer desde cualquier punto geográfico como se había abordado anteriormente lo que puede hacer más dificultosa la tarea de determinar la competencia. Todos los delitos informáticos en un primer estadio se comenten por una persona indeterminada o desconocida, motivo por el cual la labor investigativa debe ser ardua y profunda.

En el momento de la comisión de un delito informático, el delincuente va hacer todo lo posible por evitar ser encontrados o eliminar cualquier huella para evitar ser encontrados, es por eso y debido al grado de dificultad estos delitos requieren especial tratamiento a la hora de determinar la competencia.

Empecemos por el inicio, partiendo desde la comisión del delito, puede haber sido cometido en cualquier lugar del mundo o zona geográfica y puede haber sido cualquier persona, esta persona hará todo lo que esté en su alcance para no ser descubierta, aquí ya tenemos dos factores que hacen más difícil la tarea, la primera es que el delito pudo haber sido cometido en cualquier punto del mundo y la segunda es que la persona hará lo posible por no dejara rastro de su acto delictivo.

La jurisprudencia del Tribunal Supremo se ha referido al respecto como los delitos a distancia, que son aquellos que se realizan en un lugar y el resultado del hecho delictivo se obtiene en otro distinto, en esos casos, al momento de decretar la comisión del delito, se tendrá en cuenta la Teoría de la Ubicuidad que se define como el lugar de acción del delito, donde el resultado debe ponderar el lugar donde se realizó y el lugar donde el delito se consumó.

En materia de delitos informáticos, como puede ser la captación masiva de información, donde se pueden afectar diferentes personas en el mundo, este delito debe ser perseguido e investigado por cualquier de las zonas geográficas donde se haya cometido, en razón de esto el juez que primero haya iniciado las actuaciones procesales será competente para realizar las actuaciones de juzgamiento. Conforme se vaya adelantando la investigación, se podrá llegar a determinar en qué lugar se cometió el hecho delictivo.

Se debe buscar la eficacia en el campo procesal, ya que es amplia la problemática que se debe desafiar en materia de delitos informáticos, se deben afrontar mayores retos que trae consigo la globalización de la utilización de sistemas informáticos y las acciones delictivas

que van de la mano, por un lado se deben llenar las lagunas legislativas, como también se debe tener en cuenta la dispersión normativa, la amplitud geográfica, la recolección de las pruebas y los riesgos y demoras que trae consigo la investigación de un delito informático. Como lo expresa el autor Andrés Díaz López, aunque existe una cantidad innumerable de normatividad internacional en muchos procesos se sigue notando lagunas, es por ello que se debe seguir trabajando en la conformación del Derecho Procesal Penal Internacional ciberdelictual.

4.1.2. Estados Unidos

Los delitos informáticos en Estados Unidos se han considerado como uno de los ataques más poderosos en el último siglo a nivel digital, ya que últimamente estos han crecido de manera considerable haciendo que las situaciones en las cuales se encuentre en curso un delito informático se afecten sistemas de seguridad de vital importancia entre otros.

Los ataques cibernéticos están afectado cada vez más fuerte la capacidad de defensa del gobierno, lo cual es una situación de vulnerabilidad donde se pueden filtrar secretos de Estado, como también en el sector privado donde también se presencian estos ataques informáticos.

La legislación informática estadounidense posee leyes federales, las cuales resguardan de los posibles ataques a los cuales pueden ser víctimas los usuarios de los ordenadores. El "Acta Federal de Abuso computacional de 1994 (18 U.S.C. Sec 1030)", modificado por el "Acta de Fraude" y el "Acta de Abuso Computacional de 1986", la cual establece la

diferenciación de que es un virus y que no lo es, y que daños pueden realizar estos en los diferentes ordenadores en sus redes o datos y programas de información.

El Acta de 1994 diferencia dos situaciones que se pueden presentar en la realización de un delito informático : el primero es de aquellas personas que de forma temeraria lanzarían ataques de virus y el segundo, aquellas personas que realizan estos actos de manera dolosa con intención de realizar algún daño grave, el Acta establece, que para quienes de manera intencional realizan un daño por trasmisión de un virus, el castigo será de hasta 10 años de prisión más una sanción pecuniaria , y para los que realicen estas acciones de manera temeraria la sanción será entre una pena monetaria y un año de prisión.

Esta ley establece una responsabilidad más amplia en el deber de evitar el problema que causan los virus informáticos especialmente por quien los constituye ya que el accionar de un virus puede causar daños graves.

El autor Miguel Estrada Garavilla aborda que en el Estado de California se adoptó la Ley de Privacidad en la cual se contempla lo siguiente:

Los delitos informáticos, pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta Ley. Sin embargo, es importante destacar las enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en las que, entre otras, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de diez mil dólares por cada persona afectada y hasta cincuenta mil dólares el acceso imprudencial a una base de datos (Garavilla).

La sección 1029 contempla la prohibición de fraude de las actividades relacionadas con el acceso o uso de dispositivos falsificados como PINs, tarjetas de crédito, numero de cuentas entre otros identificadores electrónicos. En esta sección se establecen los siguientes delitos con sus correspondientes penas: La producción, uso o tráfico de dispositivos de accesos falsificados, su pena será de cincuenta mil dólares o dos veces el valor de la conducta ejecutada será castigado con quince años de prisión, para aquellas personas quienes reinciden en el delito la pena ser de $100.000 y la pena de 20 años de cárcel.

La tenencia de quince o más dispositivos de acceso no autorizado o falsificado, será castigado con una pena de diez años de prisión y una sanción monetaria de diez mil dólares o dos veces más del valor de la conducta criminal cometida, para aquellos quienes reincidan en el delito será de veinte años de prisión y una sanción monetaria de cien mil dólares. La ejecución de transacciones, con mecanismos de acceso que sean propiedad de otra persona con la finalidad de adquirir una suma de mil dólares o más durante un año, será castigado con una sanción de diez mil dólares y diez años de prisión , quien reincida a la comisión de este delito la pena será de veinte años de prisión y una multa de cien mil dólares.

La producción, utilización, tráfico y tenencia de mecanismos tecnológicos, que sufran alguna afectación o alteración con el fin de llevar a cabo un uso indebido de las telecomunicaciones, serán castigados con quince años de prisión más una multa de cincuenta mil dólares y quien reincida tendrá veinte años de cárcel y una sanción monetaria de cien mil dólares. También quien fabrique receptores- escaneadores, hardware o software

que se utilice para modificar mecanismos de telecomunicaciones y todos aquellos artefactos que intercepten llamadas telefónicas, tendrá una pena de quince años de prisión y una multa de cincuenta mil dólares, y quien reincida en estas acciones tendrá una pena de veinte años de cárcel y una sanción monetaria de cien mil dólares.

Por último, engañar a una persona en relación a que el delincuente pertenece a una entidad de crédito para obtener información para realizar transacciones u obtener dinero la pena será de un año y diez años de prisión si esta persona vuelve a reincidir.

La "ley sobre abuso y fraude Informático de 1986", promueve la legislación federal a las acciones delincuenciales en los ordenadores donde su intención sea de trasmitir lo que está realizando otra persona o dañar otro ordenador estas situaciones son apoyadas de forma investigativa por el F.B.I. de tal forma que maneja la investigación frente a estas actividades criminales, como se había abordado antes que es la obtención de información relacionada con asuntos de defensa nacional, o también de energía nuclear con el objetivo de dañar el país.

Otra de las acciones, de la cual se está en prevención cuando se refiere a un ataque informático, es la obtención de información de registros financieros de una institución fiscal o de un propietario de tarjeta de crédito como se había visto anteriormente, ya que estas acciones de decremento patrimonial a los usuario de estas bases electrónicas hacen perder la confianza de estos servicios sin dejar de lado el acto delincuencial de obtención de los datos financieros, como también que se ejecute un fraude mediante el acceso a un equipo de carácter federal con la finalidad de obtener algo.

La propiedad intelectual también se ha venido visto afectada por medio de acciones delincuenciales, debido a este problema se ha venido implementado con el Departamento de Justicia de los Estados Unidos sección de delitos informáticos, acciones prevención para combatir este problema, sin dejar a lado que se adelanten de manera rápida y pertinente las acciones investigativas y judiciales.

Estas acciones de alterar, destruir, duplicar, trasmitir datos, alterar el ejercicio normal de los computadores, son acciones que deben ser combatidas desde todos los ángulos, pero no basta con solo ser penalizadas también las acciones de prevención y de concientización de estas acciones delincuenciales deben ser abordadas por todas las organizaciones competentes.

Con base a lo anterior, es evidente el número de procedimientos judiciales a los cuales se exponen los delitos informáticos, estas actividades requieren un manejo acorde con relación a su competencia para que el juez pueda enjuiciar estos delitos, se han propuesto diferentes soluciones en materia técnica para poder enjuiciar de forma debida estos delitos informáticos, las acciones de conocimiento de IP como habíamos manejado anteriormente con España, permiten que los procedimientos judiciales se hagan de la mejor manera posible. El Tribunal Federal Norteamericano, manejara a que servidor le corresponde la responsabilidad cuando se vea en curso un delito informático.

Federal Computers investigation Commitee, es la organización más relevante en relación con la investigación de delitos computacionales sus investigadores son diferentes técnicos

en las materias de programadores, abogados, policías entre otros que trabajan arduamente para combatir estos delitos.

Los organismos correspondientes, deberán realizar acciones que permitan un mejor uso adecuado de las nuevas tecnologías aportando un nivel de seguridad frente al uso de las tecnologías, sin menospreciar los posibles ataques a los cuales podemos estar presentes. Es una amenaza constante que cada vez va creciendo conforme lo hace la tecnología que no es un secreto que cada día da saltos gigantescos y hay que ir de la mano con esta evolución inevitable.

5. Sujetos del Delito Informático

Dentro de la conducta punible, se genera la existencia de dos sujetos, un sujeto activo y un sujeto pasivo, además de la existencia del bien jurídicamente tutelado, razón por la cual, definiremos estas figuras de la siguiente manera:

Sujeto Activo:	**Sujeto Pasivo:**	**Bien Jurídicamente Protegido:**
Es quien planea y ejecuta la conducta punible, es un individuo que generalmente cuenta con conocimientos en materia informática los cuales facilitan la comisión de este tipo de delitos.	Es quien posee la titular sobre el bien jurídicamente tutelado por el ordenamiento jurídico y sobre quien recae la acción punible.	Bien que se ve afectado con la comisión de la conducta punible, puede generar una afectación patrimonial, a la información, datos personales, entre otros.

6. Modalidades de los delitos informáticos

Debido a la amplitud que implica la informática, existen diversidad de ilícitos que solo se ven limitados, como Camacho Losa expresa en su libro, por la relación de tres factores: la imaginación del autor, su capacidad técnica y las deficiencias de control existentes en las instalaciones informáticas. (Pino, 2008)

Sin embargo, la Organización de Naciones Unidas ha realizado un listado mínimo de delitos informáticos, que organiza según tres criterios, a saber:

- Fraudes cometidos mediante la manipulación de computadoras.
- Manipulación de los datos de entrada.
- Daños o modificaciones de programas o datos computarizados (Pino, 2008).

6.1. Principales conductas delictivas cibernéticas

Como se mencionó anteriormente los delitos cibernéticos se encuentran divididos según tres criterios, estos criterios a su vez contienen ciertas conductas que son consideradas como ilícitos a nivel internacional y que deben ser explicados para tener claridad sobre el tema.

Fraudes

- **Data diddling:** También conocida como datos falsos o engañosos o sustracción de datos, se define como una manipulación de datos de entrada al computador con el

fin de producir o logar movimientos falsos en transacciones de una empresa (Pino, 2008).

Este delito no requiere de conocimientos técnicos de informática y puede ser realizado por cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos (Pino, 2008)

- **Troya horses:** También conocido como caballos de Troya. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas, es decir, se insertan instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal. Suele pasar inadvertida pues quien comete este delito debe tener conocimiento técnico en informática (Pino, 2008).

- **Rounching Down:** La también conocida técnica del salami. Consiste en introducir al programa unas instrucciones para que remita a una determinada cuenta los céntimos de dinero de muchas cuentas corrientes (Pino, 2008).

- **Manejo de los datos de salida:** Se efectúa fijando un objetivo al funcionamiento del sistema informático. Un ejemplo de ello es el fraude realizado a través de cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos (Pino, 2008).

- **Phishing:** Se define como la obtención de información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños, es decir, su finalidad es robarle su identidad a la víctima. Este tipo de conducta se lleva a cabo a través de correos electrónicos o ventanas emergentes. El phishing cuenta con la modalidad segmentada o spear phishing en la cual se buscan grupos vulnerables de personas para atacar (Pino, 2008).

Los quebrantos o alteraciones de programas o datos sistematizados.

- **Sabotaje informático:** Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema (Pino, 2008).

- **Logic Bombs: "**Las bombas lógicas son un tipo de bomba de tiempo diseñadas para causar el máximo de daño en un cierto tiempo determinado. Esta requiere de conocimientos técnicos pues requiere la programación a futuro de la destrucción o reforma de datos, son de difícil detección y por esto es el que más daño causa

- **Gusanos:** Se fabrican al mismo tiempo que el virus y su objetivo es infiltrarse en programas legítimos de procesamiento de datos o para modificar o destruir los datos, los gusanos no pueden regenerarse y es esta característica la que lo diferencia de un virus, sin embargo, puede causar mucho daño a un sistema informático (Pino, 2008).

- **Virus informático y Malware:** Son elementos informáticos cuya tendencia es propagarse y extenderse dentro del sistema al que acceden. Poseen varias características, a saber, se pueden contagiar de un sistema a otro y poseen diferentes grados de malignidad. Estos pueden ser contrarrestados a través de antivirus, aunque algunos son muy resistentes a estos (Pino, 2008).

Ahora bien, encontramos otros tipos de delitos de gran importancia como son:

Espionaje informático y hurto de software.

- **Data Leakage:** La fuga de datos también llamada divulgación no autorizada de datos reservados, es una forma de espionaje industrial y su finalidad es la sustracción de información de una empresa (Pino, 2008).

- **Reproducción no autorizada de programas informáticos de protección legal:** También llamada piratería informática, representa una perdida económica para los legítimos propietarios (Pino, 2008).

Hurto de servicios

- **Hurto del tiempo del computador:** Corresponde a el robo de tiempo del uso de un computador (Pino, 2008).

- **Scavenging:** Es aquella en la que se aprovecha la información abandonada sin ninguna protección (Pino, 2008).

- **Piggybacking e Impersonation:** figuras en que concursan a la vez los delitos de suplantación de personas o nombres y el espionaje, entre otros delitos. En estos casos, el delincuente utiliza la suplantación de personas para cometer otro delito informático (Pino, 2008)

Acceso no autorizado a servicios no autorizados

- **Trap doors:** Introduce interrupciones dentro de la lógica de los programas para poder chequear en medio de procesos complejos, si los resultados intermedios son correctos, producir salidas de control con el mismo fin o guardar resultados intermedios en ciertas áreas para comprobarlos más adelante (Pino, 2008).

- **Wiretapping:** Consiste en interferir las líneas telefónicas de transmisión de datos para recuperar la información que circula por ellas, por medio de un radio, un módem o una impresora (Pino, 2008).

- **Hacking:** Los también conocidos piratas cibernéticos accedan de forma no autorizada, por lo general violando los mecanismos de seguridad, a los archivos y bases de datos contenidos en los sistemas informáticos ajenos, normalmente de grandes empresas o instituciones (Magariños).

- **Pharming:** Consiste en remplazar una página web por una clonada con el fin de obtener los datos que el usuario ingrese en ella (Quintero & Martin).

- **Cracking:** Es la conducta consistente en la destrucción o en la producción generalizada de daños en su sistema, datos, programas informáticos o telemáticos (Gomez M. M., 2001)

Entre otras conductas ilícitas podemos encontrar distribución de imágenes de agresión sexual contra menores, botnets (redes de equipos infectados que manejan usuarios remotos), sexting, ciberbullying (acoso por medios virtuales), cibergrooming acoso, entre tras. (González, 2013)

6.2. Guerra y terrorismo cibernético

Ciberterrorismo

Con el desarrollo tecnológico y su integración con la sociedad actual, las sociedades avanzadas han llegado a un nivel alto de dependencia del mismo, controlando procesos y actividades cotidianas a través de los mismos, por lo cual al causar daño en estos se podría llevar a un país al colapso. (Vieites)

En los años 80, Barry Collin, acuño el termino ciberterrorismo por primera vez, haciendo referencia a la convergencia del ciberespacio y el terrorismo.

Se entiende entonces el concepto de ciberterrorismo como el uso deliberado de tecnologías relacionadas con la informática para amenazar o atacar a personas, así como a propiedades

o infraestructuras, con el fin de infundir terror para alcanzar un fin político, ideológico, social o religioso. Además, se incluye en esta definición el desarrollo de la acción terrorista en el ciberespacio a través de propaganda, financiación, reclutamiento, obtención e intercambio de información, etc. (Criado & Barrego, 2016).

Estas ofensivas podrían traer como consecuencia el corte de suministro eléctrico y posible descontrol de centrales nucleares, hidroeléctricas y térmicas, el colapso de redes de comunicación y redes telefónicas, desarrollo de ataques específicos contra los sistemas de comunicaciones militares, caos financiero, intervención en el control del tráfico aéreo y ferroviario, ataques cibernéticos, destrucción de bases de datos estatales, sabotajes locales en la capital, entre otros. Los ataques que interrumpen servicios no esenciales o que son una molestia costosa no se configuran como ciberterrorismo (Sebastian, 2017)

El ciberterrorismo se caracteriza por:

- No se requiere de la figura física del terrorista.
- En caso de que el plan falle, el terrorista toma los errores para mejorar su próximo ataque sin arriesgar su vida.
- Este tipo de ataques asegura al terrorista su seguridad temporal (Orta, 2012).

No existen tipificaciones propiamente correspondientes al ciberterrorismo, sin embargo, en varios países esta conducta ya se encuentra ligada a otro tipo de delitos informáticos, un

ejemplo de ello son Venezuela, España, México y Estados Unidos, a continuación, desarrollaremos el tema brevemente. (Orta, 2012)

Guerra Cibernética: Es un área dentro de las agencias militares de los países que tienen como objetivo encontrar las vulnerabilidades técnicas de los sistemas o redes informáticas del enemigo para penetrarlas y atacarlas, tanto, así como para extraer datos e información sensible. En este caso el ciberespacio es un campo de batalla y las armas son programas o aplicaciones informáticas. (Gustavo)

Los ataques cibernéticos se determinan por dos factores por la meta y por el daño que se desee causar, algunos ejemplos de estos son:

- **Virus informáticos:** Son programas cuyo objetivo es infectar otros archivos con el objetivo de dañar un sistema informático. (Martinez, 2016)

- **Troyanos:** Consiste en introducirse en el sistema como un programa aparentemente inofensivo, siendo verdaderamente un programa que permite el control remoto de dicho sistema. Al igual que los virus, pueden modificar, eliminar ciertos ficheros del sistema y a mayores pueden capturar datos confidenciales y enviarlos a una dirección externa (Alvarez & Cocheiro)

- **SPAM:** Se define como los mensajes no solicitados, habitualmente de tipo publicitario, enviados en forma masiva a muchos usuarios al mismo tiempo. La vía

mas utilizada es la basada en el correo electrónico, pero puede presentarse por programas de mensajería instantánea o por teléfono (Facua).

- **Instalación de virus espías o keyloggers:** Es un programa cuya función es guardar la pulsación de teclas (Martinez, 2016).

- **Uso de Rootkits:** Herramientas que permiten camuflar el acceso a un programa ilícito, este oculta procesos y archivos, estos no pueden ser detectados. (Martinez, 2016)

- **Uso de archivos BOT del IRC (Internet Relay Chat):** Programa que permite el control remoto de un sistema sin el conocimiento del usuario (Martinez, 2016)

- **Interferencia electrónica de comunicaciones:** Consiste en alterar un circuito, componente o sistema electrónico causada por una fuente de radiación electromagnética externa al mismo. Esta perturbación puede interrumpir, degradar o limitar el rendimiento del sistema, causando así interferencias con el propósito expreso de producir una disfunción en los sistemas de comunicaciones (Martinez, 2016)

- **Blind Radars:** Tecnica de interferencia en los radares de las torres de control y en los sistemas de rastreo de los aviones de forma electrónica (Martinez, 2016).

6.3. Delitos informáticos en particulares

En la actualidad, la creciente demanda de herramientas que faciliten la comunicación mundial entre particulares, y en especial el avance de diversas redes sociales, usadas por millones de personas a nivel mundial, hace que el consumo creciente de este tipo de plataformas que facilitan las tareas diarias de millones de personas en el mundo, genere una desprotección en cuanto a la seguridad digital de los usuarios y consumidores de estos instrumentos informáticos, toda vez que la falta de conocimiento principalmente frente a las medidas de seguridad aplicables sobre los datos que los particulares manipulan diariamente en redes, junto con las fallas en los sistemas de seguridad que poseen estas plataformas, sirven de medio para facilitar a diversos individuos, con intenciones delictivas, la ejecución y comisión de estas conductas.

Por lo anterior, se observa que, como conductas cibernéticas delictivas, de las cuales los particulares son frecuentemente víctimas encontramos principalmente las siguientes:

Ciberbullying: Se entiende como cualquiera de las posibilidades de uso de las nuevas tecnologías de la información y de la comunicación para hostigar con ensañamiento a su victima. (Quezada)

Pornografía Infantil: son innumerables los casos de pornografía infantil que se ejecutan globalmente y de manera continua en la web, toda vez que este medio permite el acceso de una manera más facil de material inormático que contenga imagénes, videos de menores, toda vez que con la utilización de diversas herramientas y mecanismos informáticos resulta

mas facil atraer la atención de los menores, desencadenando estas actuaciones un problema de proporciones inimagibales en relación a la protección de niños, niñas y adolescentes.

Phishing: también conocido como suplantación de identidad, es una conducta delictiva con la cual se busca obtener información bancaria de una persona de manera fraudulenta, la cual se ejecuta cuando el phiser obtiene esta información valiéndose de engaños electrónicos para suplantar principalmente entidades de confianza, por medio de comunicaciones informáticas, que le permitan acceder a esta información.

Hurto de información: esta figura es una de las más utilizadas por los delincuentes informáticos, ya que por el descuido constante de la información por parte de los usuarios de internet en los diversos campos de interacción informática, facilitan a los delincuentes la obtención y aprovechamiento de dicha información, lo cual puede desencadenar la comisión de otros delitos como secuestros, extorsión, hurtos presenciales, entre otros.

6.4. Delitos informáticos en el Estado.

El tema que nos ocupa dentro de este acápite, es la relación de delitos informáticos, que atacan y ponen en peligro la seguridad de los diversos gobiernos alrededor del mundo. Por lo cual entraremos a analizar principalmente dos de ellos que son la fuga de información, o el hurto de información a estos sistemas de seguridad gubernamentales, y también los diversos ataques por medio de la utilización de virus o malware, que pone en riesgo el funcionamiento y la seguridad de estos sistemas de protección de información implementados por los Estados a nivel mundial, por lo anterior es importante destacar tres

de los casos más sonados y discutidos que afectaron estos medios de protección, y que pusieron principalmente al descubierto información con etiqueta confidencial de los Estados a nivel mundial, y también generaron daños informáticos y los sistemas operacionales de estos entes.

Por lo anterior para el desarrollo del presente acápite es importante tener en cuenta las siguientes definiciones:

Fuga de Información: es la perdida de la confidencialidad, de forma que: información que no deberia ser conocida más que por un grupo de personas, en el ámbito de una organización, área o actividad, termina siendo visible o accesible para otros (INTECO)

Daño informático: De conformidad con lo establecido en la ley 1273 de 2009 artículo 269D, el daño informatico se tipifica como delito cuando una persona destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos. (ley 1273 de 2009, 2009)

Malware o virus : Programa malicioso que infecta a otros archivos del sistema con la intención de modificarlo o dañarlos. Dicha infección consiste en incrustar su código malicioso en el interior del archivo víctima, normalmente un archivo ejecutable, de forma que a partir de ese momento dicho ejecutable pasa a ser portador del virus y por tanto, una nueva fuente de infección (Azamar)

- **Wikileaks:** es uno de los casos de filtración de ifnromación más grande y sonado del mundo, toda vez que diversos gobiernos principalmente el norteamericano, fueron víctimas de filtración de información, que fue publicada a través de una diversidad de periodicos de gran relevancia a nivel mundial, vulnerando de esta manera el esquema de seguridad de los Estados Unidos, y demás gobiernos.

- **Panama Papers:** Todo inició a finales de 2014, cuando el periodista Bastian Obermayer del diario alemán Süddeutsche Zeitung de Múnich, fue contactado por una fuente anónima vía correo electrónico, con la intención de librear documentos del escritorio jurídico panameño Mossack Fonseca, Bufete de abogados que desde su sede principal y mediante sus 38 sucursales en todo el mundo, lidera la industria de incorporación de empresas en paraísos fiscales como: Las Islas Vírgenes Británicas, Panamá, Seychelles, Samoa, Bahamas, Anguila, Nevada, Hong Kong, Reino Unido, Belice, Costa Rica, Wyoming, Malta, Nueza Zelanda, Chipre, Niue, Uruguay, Ras Al Khaimah, Singapore, Isla de Man y Jersey. Anónimo ofrecimiento al que Obermayer juto con su colega Frederick Obermaier, decidieron aceptar. Desde entonces comenzó a tejerse toda una estrategia de suministro de información de forma encriptada entre la fuente y los periodistas. La fuente fue liberando datos por entregas a lo largo de diez meses. Su última actualización fue en marzo de 2016, lo que dejo al descubierto un total de 2,6 terabytes de datos, es decir, 11.5 millones de documentos, entre los que se cuentan: correos electrónicos, formularios financieros, pasaportes y registros corporativos; que revelan casi 40 años de registros. (Ascanio)

- **WannaCry:** Este ataque en particular aprovechó una vulnerabilidad de los sistemas operativos de Microsoft, entre ellos los Microsoft Windows 7, 8.1, y 10, así como Microsoft Windows Vista SP2 y Server 2008/2012/2016 que no contaban con la actualización necesaria para corregir la vulnerabilidad que el malware aprovechó. Después de captar los recursos, las direcciones permanecieron sin movimientos hasta el día 03 de agosto de 2017. (Macedo & Rosales, 2017)

CAPÍTULO II. DELITOS INFORMÁTICOS EN COLOMBIA.

1. Ciberdelincuencia en Colombia.

De conformidad con el fuerte avance que ha tenido el desarrollo y ejecución de los delitos informáticos a lo largo del mundo, como lo pudimos ver anteriormente, donde resumimos tres de los ataques más sonados, y que han generado una afectación de carácter global, en el siguiente título daremos a conocer la dinámica con la que funciona el Cibercrimen en nuestro país, desarrollando de esta manera las estadísticas presentada por Centro Cibernético Policial, principalmente para los años 2014, 2015, 2016, 2017.

1.1. Estadística poblacional de ataques cibernéticos en Colombia.

De conformidad con lo expuesto dentro del informe titulado Amenazas del Cibercrimen en Colombia 2016-2017, en los últimos 3 años se recibieron por medio del Centro Cibernético

Policial 15.565 incidentes informáticos (Policia Nacional, Centro Cibernético Policial , 2017)

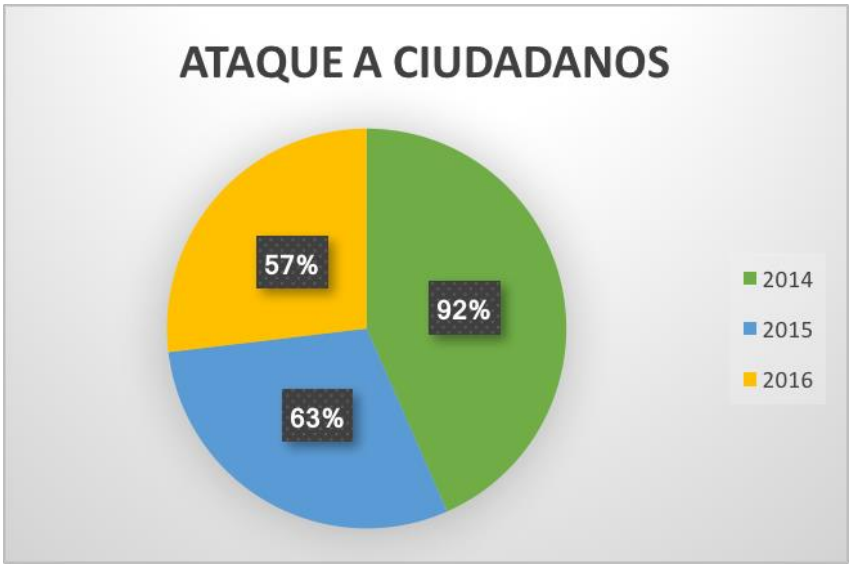
A partir de la caracterización dada en el mencionado informe, los delitos informáticos en Colombia se ejecutan principalmente de la siguiente manera:

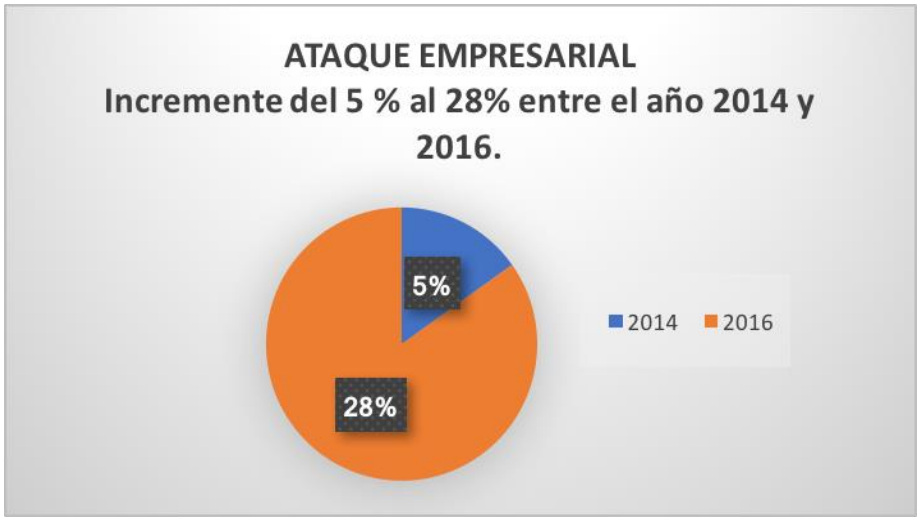
1. Se configura según lo expuesto en el informe titulado Amenazas del Cibercrimen en Colombia 2016-2017 un cambio en la escogencia de las personas afectadas por la ejecución de delitos informáticos, pasando de tener a particulares como las principales víctimas, a afectar grandes empresas tanto privadas como públicas, que generan una mayor ganancia para los ciberdelincuentes.

Por ende, se tiene la siguiente información:

El 92 % de las conductas delictivas en 2014, afectaba a particulares del común, en el 2015, tal afectación a ciudadanos era del 63% y en el 2016 del 57%, presentando una notable disminución en la afectación a ciudadanos del común.

Por otro lado, en el campo empresarial, se dio un incremento del 5% a un 28% que de manera gráfica se pueden ver de la siguiente manera:





2. Se emplean nuevas herramientas de comercio electrónico con la finalidad de realizar estafas por la modalidad del phishing, teniendo en cuenta que una de las principales afectaciones a la ciudadanía se genera por la publicación de falsas ofertas, publicadas en internet. (Policia Nacional, Centro Cibernético Policial , 2017)

3. La utilización de entes gubernamentales como mecanismo para realizar la propagación de malware o virus. En relación a este punto encontramos que por medio de correos electrónicos se utilizó en nombre de instituciones como la Fiscalía General de la Nación, DIAN y el SIMIT, para captar la atención de las victimas, permitiendo al delincuente ejercer control sobre el ordenador afectado y la obtención de la información deseada. (Policia Nacional, Centro Cibernético Policial , 2017)

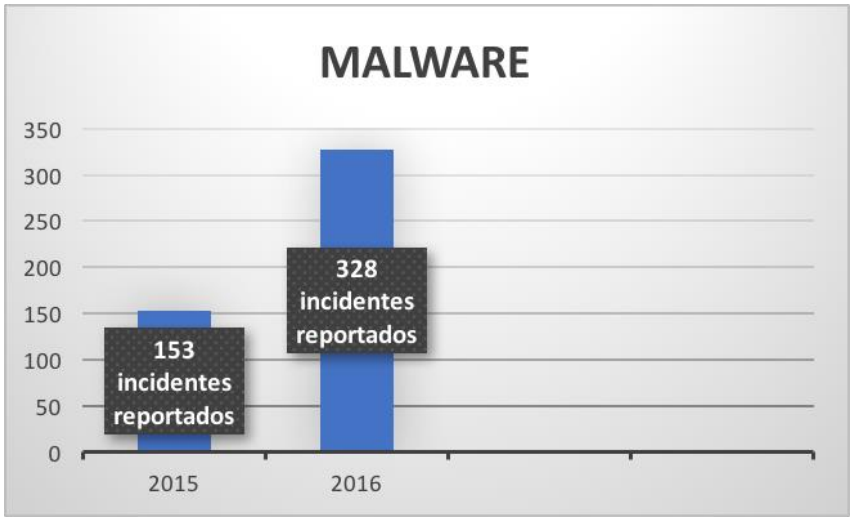
Por lo anterior es importante resaltar que estos ataques se generan principalmente por medio de Malware, APT y Ransomware, frente a lo cual encontramos los siguientes datos:

- En relación con los ataques de malware se genera un incremento del 114.4% que se ve reflejado de la siguiente manera:

  2015: 153 incidentes reportados

  2016: 328 incidentes reportados (Policia Nacional, Centro Cibernético Policial , 2017)

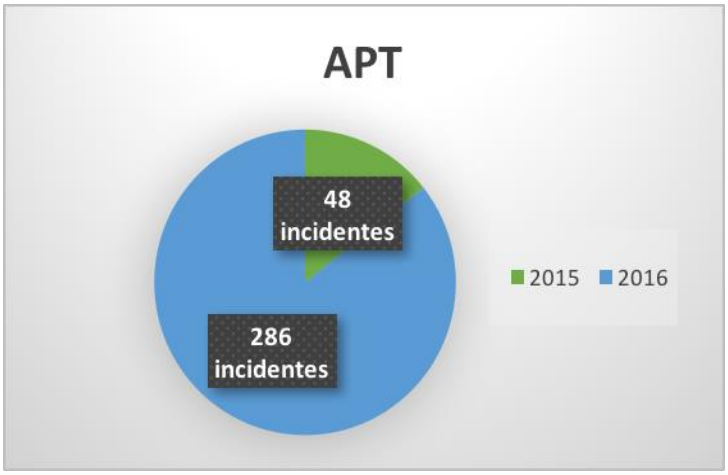
  Información que de manera gráfica se ve reflejada de la siguiente manera:



- Las ATP (Amenazas Persistentes Avanzadas) recibieron los siguientes datos:

  2015: 48 incidentes

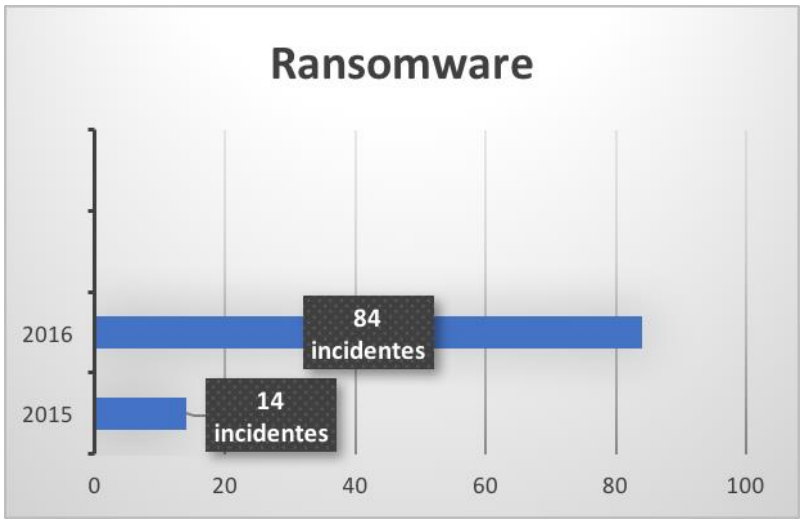
  2016: 286 incidentes (Policia Nacional, Centro Cibernético Policial , 2017)



- El Ransomware tuvo un incremente del 500%, expuesto de la siguiente manera:

  2015: 14 incidentes

2016: 84 incidentes (Policia Nacional, Centro Cibernético Policial , 2017)



4. Utilización de internet como herramienta de intimidaciones y provocación a la comisión de conductas delictivas. Aunque internet es un medio por medio del cual gozamos de infinidad de funciones que nos hacen mucho más fácil el día a día, y que nos ofrece muchas alternativas, relacionadas con entretenimiento, información, material educativo, redes sociales entre otros, en muchas ocasiones también es un mecanismo utilizado para ejecutar diversas conductas delictivas. (Policia Nacional, Centro Cibernético Policial , 2017)

En relación con lo anteriormente expuesto, es importante resaltar el siguiente tema desarrollado en el informe presentado por el Centro Cibernético Policial, el cuales se trata de los principales delitos denunciados en nuestro país.

- **Principales delitos denunciados**. Ya que la finalidad del presente punto es dar a conocer la estadística poblacional de los ataques cibernéticos en Colombia, procederemos a exponer los datos presentados en el presente informe, por medio de gráficos que nos generen una claridad acerca de los principales delitos que afectan a nuestra nación. (Policia Nacional, Centro Cibernético Policial , 2017)

  Es importante recordar en este punto que la ley 1273 del año 2009, "por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones", (ley 1273 de 2009, 2009) se tipifican las siguientes conductas delictivas:

  Artículo 269A Acceso abusivo a un sistema informático

  Artículo 269B Obstaculización ilegítima de sistema informático o red de telecomunicaciones

  Artículo 269C Interceptación de datos informáticos

  Artículo 259D Daño informático

  Artículo 269E Uso de software malicioso

  Artículo 269F Violación de datos personales

  Artículo 269G Suplantación de sitios web para capturar datos personales

  Artículo 269H Circunstancias de agravación punitiva.

Artículo 269I Hurto por medios informáticos y semejantes

Artículo 269J Transferencia no consentida de activos (ley 1273 de 2009, 2009)

Por lo anterior tenemos que, durante los años 2014, 2015, 2016 y 2017 según el informe referenciado, se recibieron 13.774 denuncias por violación a la ley 1273 de 2009. (Policia Nacional, Centro Cibernético Policial , 2017)

De acuerdo a la anterior información, encontramos el siguiente ranking con los 3 delitos que se ejecutan con mayor frecuencia:

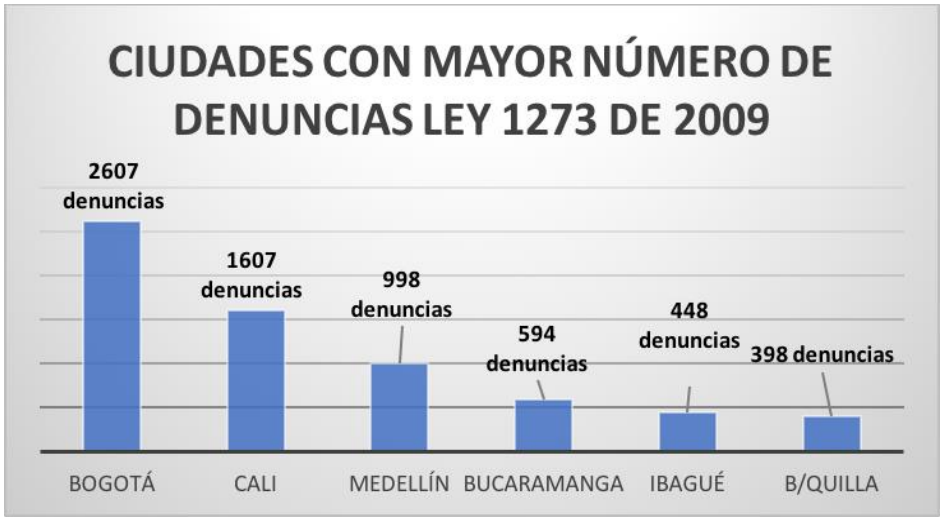
Artículo 269I Hurto por medios informáticos y semejantes	68%
Artículo 269A Acceso abusivo a un sistema informático	13%
Artículo 269F Violación de datos personales	12%

(Policia Nacional, Centro Cibernético Policial , 2017)

Es importante resaltar que las ciudades en las que se presentan un mayor número de reportes de incidentes informáticos se mostraran de la siguiente manera:

(Policia Nacional, Centro Cibernético Policial , 2017)

Por otro lado, las ciudades donde se evidencia una mayor cifra de denuncias por la ley 1273 de 2009, son:



(Policia Nacional, Centro Cibernético Policial , 2017)

CAPÍTULO III. ANÁLISIS JURISPRUDENCIAL DE LOS DELITOS INFORMÁTICOS

1. Análisis jurisprudencial desde el ámbito internacional

Dentro del presente punto, entraremos a realizar un análisis en relación a la jurisprudencia generada en el ámbito internacional, resaltando de esta manera los principales puntos que nos sirvan de referencia, para continuar con el desarrollo del presente trabajo, por ende, este tema lo abordaremos de la siguiente manera:

1.1. Convenio sobre ciberdelincuencia, Budapest 23 XI 2001.

Este Convenio fue expedido por el Consejo de Europa en 2001. Y cuenta con un protocolo adicional fijado en el año 2003, "la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos".

Este convenio consta de cuatro (4) capítulo y cuarenta y ocho artículos (48)

1.2. Protocolo Adicional a la Convención sobre la Delincuencia Cibernética, sobre la criminalización de actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos.

Complementando el Convenio de Budapest , se promulga un protocolo adicional del año 2003, sobre la incriminación de actos de naturaleza racista y xenófoba que viene a completar al anterior, toda vez que esta temática esta claramente relacionada con los delitos cometidos por vía informática, tratando de complementar y fortalecer la lucha contra este tema a través de internet.

1.3. Directiva 2002/58/EC relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

Se dispone dentro de la Directiva lo siguiente: La presente Directiva armoniza las disposiciones de los Estados miembros necesarias para garantizar un nivel equivalente de protección de las libertades y los derechos fundamentales y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas en la Comunidad. (Parlamento Erupeo y del Consejo, 2002)

Esta directiva consta de 21 artículos.

1.4. Decisión Marco del Consejo 2005/222/JAI relativa a los ataques contra los sistemas de información.

Esta decisión tiene como finalidad fortalecer la colaboración de los entes judiciales, y demás autoridades competentes de los distintos Estados miembro, mediante el ajuste y modificación de las leyes penales, en temas relacionados con la ciberdelincuencia.

Esta decisión se compone de 13 artículos.

1.5. d Penal de estados unidos, caso EE. UU vs Edward Snowden

En el 2013, el experto en computación y previo administrador de sistemas de la CIA Edward Snowden reveló documentos confidenciales del gobierno a la prensa sobre la existencia de programas de vigilancia gubernamentales. Según expertos legales y el Gobierno Estadounidense, las acciones de Snowden violaron el Decreto de Espionaje de 1917 el cual identifica la divulgación de secretos de estado como un acto de traición. A pesar de haber violado la ley, Snowden argumentó que tenía una obligación moral para actuar. Justificó sus acciones como "soplón" declarando que tenía el deber de "informar al público sobre aquello que se hace en su nombre y aquello que se hace en su contra." De acuerdo a Snowden, las violaciones de privacidad hechas por el gobierno tenían que ser expuestas sin importar la legalidad (Andrew)

Para el gobierno estadounidense, se cometieron los delitos de hurto, espionaje y traición a la patria.

Posición de Estados Unidos: En relación a la posición que defiende el Gobierno estadounidense, sus argumentos son basados, en que dichas actuaciones y la existencia de este tipo de programas informáticos, se desarrollan y ponen en funcionamiento por la necesidad de proteger al país de la posible comisión de actos terroristas y de la misma manera espionaje a los sistemas de seguridad del gobierno, pero aunque la postura del Gobierno Norteamericano se basa en que Edward Snowden cometió los delitos de hurto,

espionaje y traición a la patria, y que por este motivo debe ser castigado, claramente también hay una vulneración del derecho a la intimidad de las personas afectadas, y de la libertad de expresión hacia Edward Snowden.

1.6. Corte Penal de estados unidos, caso EE. UU vs Julian Assange

Esta página fue creada en el año 2006, y se definió como una organización sin animo de lucro, dentro de la cual, las personas sin ningún tipo de censura tenían la posibilidad de publicar cualquier documento, y en la cual se protegía la identidad de las personas permaneciendo en anonimato, el único requisito que estipulaba Wikileaks, se basaba en que la información publicada debía ser autentica.

En el año 2007, esta página, de conformidad con su característica de anonimato dio a conocer una serie de información relacionada con temas sensibles del Gobierno de Kenia, principalmente, temas de corrupción.

Pero la filtración mas grande e importante de información se llevó a cabo en el año 2010, cuando la página publico una serie de documentos y videos que comprometían información sensible y de carácter confidencial perteneciente al gobierno estadounidense.

Postura de Estados Unidos: Estados Unidos inició una investigación penal en contra de Julian Assange y en contra de Wikileaks a comienzos de 2010, investigación que aún sigue en pie. (Bosch, 2015)

2. Análisis jurisprudencial desde el ámbito nacional

2.1. Sentencia sp1245-2015 de 11 de febrero de 2015

Datos Generales: Radicado: SP1245-2015 Corte Suprema de Justicia Sala de Casación Penal Accionante: Carlos Arturo Álvarez Trujillo
OPINIÓN: De conformidad con el fallo emitido, la presente opinión se encuentra de acuerdo con los argumentos expuestos toda vez que, no se realizó una aplicación de la rebaja de pena, en relación a la reparación integral realizada por CARLOS TRUJILLO ÁLVAREZ, no obstante que se habían cumplido todos los requisitos para acreditar el beneficio de rebaja de pena, ya que erróneamente uno de los argumentos se basaba en que, al presuntamente no atentar contra el patrimonio económico, sino al tratarse de una afectación a los datos personales y la información, no configuraría dicho beneficio así se haya cumplido con los requisitos necesarios para efectuar la reparación integral, argumento que como se indicó, es erróneo, toda vez que en el presente caso con la afectación a la información y datos personales, también se genera una afectación al patrimonio de la víctima por ende la aplicación del beneficio de rebaja de pena es viable y es justamente aplicado en el presente caso.

2.2. Sentencia T 550-12

DATOS GENERALES: Sentencia T 550-12 Acción de Tutela Accionante: Federico José Linero Mesa Accionado Universidad Colegio Mayor de Nuestra Señora del Rosario
OPINIÓN: En relación con lo expuesto dentro del presente fallo, ésta opinión se encuentra parcialmente de acuerdo con el fallo generado, toda vez, que en relación al derecho a la libertad de expresión, expuesto dentro del presente caso, el accionante mediante un actuar grosero, y al expresar públicamente de una manera no apropiada su opinión frente a la situación que se estaba desarrollando dentro de la Universidad, puedo generar una afectación mínima frente al buen nombre de esta y de algunos de los funcionarios que allí laboran, teniendo en cuenta, que en relación con el trámite adelantado, contaba con los medios idóneos para exponer su punto de vista frente a las autoridades respectivas, pero también es importante, mencionar que se debe considerar el grado de influencia con el que contaba el estudiante dentro de la mencionada red social, para generar una afectación de tal magnitud que perturbara gravemente y de manera irreversible el buen nombre de la institución educativa y de los funcionarios involucrados, por ende se considera que la sanción asignada, es exagerada, teniendo en cuenta, los factores de influencia y distribución de la información, que una persona del común sin ningún tipo de imperio y dominio dentro del marco de las redes sociales puede generar como se manifiesta en el presente caso.

2.3. Sentencia T-277/15

DATOS GENERALES: Sentencia T-277/15 Accionante: Gloria Accionada: Casa Editorial el Tiempo
OPINIÓN: Respecto al presente caso, y al existir un conflicto de derechos de la accionante, frente a la libertad de expresión, de conformidad con el artículo publicado por la Casa Editorial El Tiempo. El presente concepto de encuentra en desacuerdo, de manera parcial con el fallo emitido por la Corte, ya que al analizar la mejor alternativa para salvaguardar los Derechos de la accionante, y también garantizar el derecho a la información, la Sala estima que "debe ordenarse al medio de comunicación que proceda a hacer uso de una herramienta técnica como "robots.txt", "metatags" u otra similar, para evitar que por medio de los buscadores de internet pueda accederse a la noticia que narra la captura y procesamiento de la accionante medida que resulta menos nociva al derecho a la información, que ordenar la eliminación de la noticia de la red; medida que debía ser acompañada de la actualización de la noticia objeto del conflicto. Pero el punto de desacuerdo se basa en que, la Corte trae como referencia la Sentencia T 040 de 2013, en la que se resolvió un caso similar a este. Se determinó allí que: "(…) en el caso concreto, el responsable de la información emitida, y por ende de su posible

rectificación, es el medio de comunicación que recolectó, analizó, procesó y divulgó la noticia, es decir, la casa Editorial El Tiempo, a través de su página electrónica oficial. En ese orden a quien procede realizar la rectificación, en caso dado, es a esta entidad. Por el contrario, para la Sala de Revisión, Google Colombia S.A. no es responsable de la noticia "Los hombres de la mafia de los llanos", pues como bien lo explicó esta empresa en el escrito de contestación, Google presta un servicio de búsqueda de la información que hay en toda la red, y no es quien redacta o publica tal información, sino que es un simple motor de búsqueda al cual no se le puede endilgar la responsabilidad sobre la veracidad o imparcialidad de un respectivo artículo, noticia o columna que aparezca en sus resultados (Sentencia T 040 de 2013, 2013)

Donde se puede evidenciar que Google Colombia S.A. al no ser quien redacta ni publica tal información, sino que simplemente es un motor de búsqueda, según la Corte no tiene ningún tipo de responsabilidad dentro del presente caso, porque básicamente no es quien produce la información, punto en el cual se debe tener en cuenta que Google, en el continente Europeo, está en la obligación de borrar la información obtenida en su buscador, cuando se genere una vulneración de los Derechos de alguna persona.

Medida que se considera también debería ser adoptada en el caso objeto de estudio ya que la corte está dando una solución incompleta a la petición de la accionante, toda vez que Google Colombia S.A., tiene una responsabilidad ya que así no produzca la información, si posee en sus bases de datos, información sobre las publicaciones y noticias que se divulgan como también posee datos de los usuarios de su buscador, siendo una inexactitud manifestar que Google no tiene ningún tipo de responsabilidad, ni debe adoptar medidas sobre el presente caso.

2.4. Sentencia C334 de-2010

DATOS GENERALES: Sentencia C334 de 2010 Demandante: Alexander Díaz García Magistrado Ponente: Dr. Juan Carlos Henao Pérez
OPINIÓN: De conformidad con el fallo, emitido por la Corte, el presente concepto se encuentra en desacuerdo, por lo anterior, se hará un pronunciamiento primero, en relación al artículo 237, inciso 1 de la ley 906 de 2004, Frente a lo cual tenemos que debe existir un tratamiento de especial cuidado frente al material obtenido de medios electrónicos, toda vez que estos fácilmente pueden sufrir una modificación o alteración en el momento de su extracción si no se siguen ciertos lineamientos, como la aplicación de la copia espejo, estampado cronológico o hash, que busca resguardar de manera íntegra la información que contienen estos medios electrónicos, para ser evaluados dentro de un proceso, por ende, si no se llevan a cabo este tipo de instrucciones, no se garantiza un adecuado tratamiento de estos y por consiguiente no serían los medios de prueba idóneos para ser presentados dentro de un proceso, por tal razón, el accionante tiene razón al considerar y solicitar que esta evidencia no deba ser puesta ante el juez de control de garantías después de ser recolectada, sino antes, cuando se ha realizado la respectiva cadena de custodia por parte de la policía judicial, todo esto, en busca de efectuar una protección integral de los datos que allí se depositan y garantizar la adecuada extracción y estudio del material probatorio seleccionado para el caso correspondiente.

Por otro lado, Sobre el artículo 245 del CPP, también debe existir un control previo por parte del juez de control de garantías. Toda vez que no se puede generar una simple autorización a los funcionarios de policía judicial, emitida por parte del Fiscal del caso, para realizar exámenes de ADN, sobre impresiones encontradas en el lugar de la inspección. Ya que se hace referencia a datos que tienen la connotación de sensibles, los cuales deben tener un tratamiento especial, datos frente a los cuales, la manipulación ejercida, solo puede ser autorizada por su titular, o por la autoridad judicial correspondiente, situación que se garantizaría en el presente asunto con un control previo ejercido por el Juez de control de garantías en los casos en los que se ejecute la situación expuesta.

CAPÍTULO IV PROPUESTA ASIGNACIÓN DE COMPETENCIA PARA OPTIMIZAR LA IDONEIDAD DE LOS JUECES PENALES MUNICIPALES.

1. Formación del Juez en el ámbito de los delitos informáticos.

Es importante resaltar en el presente asunto a tratar, que en Colombia, la ley 1273 del año 2009 establece que los encargados de conocer de los delitos informáticos son los jueces municipales, situación que en la ley mencionada no tiene ningún tipo de desarrollo adicional, por ende, por medio la siguiente propuesta, se quiere dar a entender, que la manifestación de las conductas delictivas por medios informáticos, ha venido incrementando con el transcurso del tiempo, y en la actualidad el uso de medios informáticos para la realización de tareas cotidianas tanto en particulares como para

entidades estatales, es completamente necesario e indispensable, ya que permiten ejecutar las diferentes ocupaciones de una manera más eficiente y mucho más rápida, pero así mismo, la mayoría de usuarios de este tipo de herramientas, no cuentan con el conocimiento suficiente, para prevenir la ejecución de conductas delictivas, y debido a este desconocimiento, los equipos o medios electrónicos, son más vulnerables a sufrir un ataque cibernético.

Esta referencia es importante toda vez que, esta propuesta se centra en que los jueces, conocedores de los delitos informáticos que se ejecutan en nuestro país, deben ser profesionales con una capacitación mínima en el tema que van a desarrollar, que en este caso es toda la temática relacionada con los delitos informáticos, toda vez que la afectación que se genera con la ejecución de las conductas delictivas recae sobre los datos e información tanto de personas particulares como entes estatales, afectando de esta manera su patrimonio, buen nombre, derecho a la privacidad, entre otros aspectos, es por esta razón que el tratamiento que se le debe dar a este tipo de conductas, debe ser sumamente cuidadoso, teniendo en cuenta la pulcritud y el tacto con que debe darse el tratamiento de la evidencia dentro de los casos que sean objeto de estudio en nuestro país, es por tal razón que la propuesta que se presenta concluye en que el profesional encargado de conocer de este tema debe poseer los conocimientos mínimos tanto técnicos como teóricos en relación a la delincuencia informática, como también establecer y saber diferenciar el valor que tiene la información de las personas, toda vez que a modo de ejemplo no es lo mismo la afectación que se puede generar a una actriz o modelo de reconocimiento mundial, sobre la cual se realice una filtración de un video intimo por medio de internet, a la filtración de algún tipo de información personal que pueda sufrir una persona del común sin ningún tipo

de influencia en el mundo digital y social, por ende es importante capacitar a los jueces conocedores de este tipo de delitos, repetimos, tanto en el aspecto técnico y teórico, como en la determinación del valor de la información de las diferentes personas que puedan ser afectadas por la ciberdelincuencia.

1.1. Competencia territorial

Como competencia territorial, según lo expuesto por la Corte Constitucional en la sentencia T 308 de 2014, se tiene que el factor territorial para asignar competencia es aquella designación de juez que, de entre los que están en su mismo grado, su sede lo haga el más idóneo o natural para el caso en concreto. El criterio principal es la territorialidad o la vecindad en donde se encuentren los elementos del proceso, personas o cosas". (Sentencia T 308 de 2014, 2014)

Por tal razón se está de acuerdo en el presente punto, con lo expuesto dentro del artículo 43 de la ley 906 del año 2004 el cual establece lo siguiente:

"ARTÍCULO 43. COMPETENCIA. *Es competente para conocer del juzgamiento el juez del lugar donde ocurrió el delito.*

Cuando no fuere posible determinar el lugar de ocurrencia del hecho, este se hubiere realizado en varios lugares, en uno incierto o en el extranjero, la competencia del juez de conocimiento se fija por el lugar donde se formule acusación por parte de la Fiscalía General de la Nación, lo cual hará donde se encuentren los elementos fundamentales de la acusación.

Las partes podrán controvertir la competencia del juez únicamente en audiencia de formulación de acusación.

Para escoger el juez de control de garantías en estos casos se atenderá lo señalado anteriormente. Su escogencia no determinará la del juez de conocimiento." (Ley 906 de 2004 Por la cual se expide el Código de Procedimiento Penal)

Toda vez que en relación a la temática de delitos informáticos, el juez competente para conocer del delito debe ser aquel donde ocurrió el delito, y en los casos en que no se pueda determinar, se acogerá lo expuesto en el mencionado artículo, precisando que el desacuerdo radica en que por las razones expuestas en el punto anterior y debido al tratamiento especial con el que debe contar este tipo de conductas no deberían conocer en todos los casos de este tema los jueces penales municipales, sino por el contrario deberían conocer de este tema los jueces penales del circuito.

1.2. Competencia funcional

De conformidad con lo establecido por la sentencia ya referencia, de la Corte Constitucional T 308 de 2014, se entiende por competencia funcional "*la llamada competencia vertical en contraposición a la horizontal que se presenta en el factor territorial, y comprende tanto la competencia por grado como según la etapa procesal en que se desenvuelva. También se encuentra en este factor de competencia los denominados recursos extraordinarios de casación y revisión"* (Sentencia T 308 de 2014, 2014).

Por lo anterior, y en concordancia con lo que aquí se plantea, no en todos los casos los jueces penales municipales deberían conocer de los procesos relacionados con delitos informáticos, ya que como fue mencionado, es importante establecer el valor de la información que se ve afectada con la ejecución de este tipo de conducta, toda vez que esta información no puede ser calculada de la misma manera, ya que nuevamente ponemos como ejemplo no es lo mismo el valor de la información hurtada a una persona del común a la información hurtada a una entidad empresarial, por tal razón es importante determinar el valor de la información objeto de litigio, para realizar una adecuada asignación de competencia al juez correspondiente.

1.3. Competencia en razón la cuantía

En relación a la competencia por razón de la cuantía de conformidad con lo establecido en la ya referencia sentencia T 308 de 2014, El factor objetivo de competencia dentro del cual se desarrolla este aspecto se define como *"aquel criterio que sirve para especializar las áreas de la jurisdicción: penal, civil, administrativa, etc., por eso es llamada en razón al litigio dada por el proceso y la cuantía. En razón a la cuantía se refiere al costo del proceso en cuanto a lo reclamado en la petición y el valor de la diferencia entre lo reclamado y lo concedido".* (Sentencia T 308 de 2014, 2014).

Teniendo en cuenta este punto, nuevamente se reitera la posición referente al valor que se debe asignar a la información que sea objeto de afectación por la ejecución de conductas delictivas por medios informáticos, ya que dicha determinación, sería relevante para la

correcta asignación del juez competente para conocer del caso, teniendo en cuenta como elementos adicionales y de igual importancia, el grado de capacitación que deben tener los profesionales conocedores de este tipo de casos, y el tratamiento adecuado y cuidadoso que debe tener la evidencia recaudada de estos medios informáticos, elementos que deben fusionarse a la asignación del valor de la información afectada, con el ánimo de generar una mayor efectividad y definición en el tratamiento de los procesos asignados a los profesionales competentes, en los que se desarrolle la ciberdelincuencia, y determinar de acuerdo a lo anterior la cuantía aplicable a los casos que se presenten.

2. Análisis de los derechos vulnerados desarrollados en la investigación

2.1. Derecho a la defensa

Se considera que existe una vulneración al Derecho a la Defensa, en el sentido en que la persona encargada de conocer el caso, debe ser una persona capacitada, con conocimientos mínimos en el tema de delincuencia informática, con la finalidad de proteger este Derecho a la Defensa, principalmente con la preservación, y el cuidado especial con que debe contar la extracción del material probatorio que se va a controvertir a lo largo del proceso, ya que si no se adoptan estas garantías mínimas por parte del órgano judicial, se estaría estructurando una vulneración clara al Derecho en discusión, toda vez que la persona encargada del caso no sería la idónea para conocer de este, ya que no contaría con la preparación mínima tanto teórica como técnica en el manejo de delitos informáticos, y por ende, se generaría la vulneración no solo de este Derecho, sino de otros más a lo largo de las distintas instancias procesales.

Adicional a esto como se indica en el segundo concepto, el sindicado tiene derecho a una defensa tanto material como técnica, y en cuanto a la defensa técnica, tiene la posibilidad de asignar un abogado de confianza, o por el contrario, se realizará la asignación de un defensor público, por ende, se considera también que aquellos abogados que ejerzan como defensores públicos dentro de un proceso, también deben contar con la debida capacitación en relación con delitos informáticos, con la finalidad de poder proporcionar a su representado, una defensa completa, en relación con la argumentación y manejo del material probatorio que se va a presentar dentro del proceso, aportando de esta manera todas las garantías con que debe contar el sindicado a lo largo del desarrollo del caso objeto de litigio.

2.2. Derecho a la igualdad

Este es un Aspecto que resulta de especial observancia, ya que este principio de igualad, busca crear un sistema jurídico diferente para quienes se encuentren en situación de desigualdad en diferentes campos, por ende en el asusto que nos atañe, es importante garantizar la protección de este Derecho de Igualdad, estructurando, de manera más eficiente y de una forma que se adapte a la evolución social y a las necesidades que se viven día a día la legislación concerciente al tema de ciberdelincuencia.

Empezando, por modificar aquella asignación relacionada, con que los jueces penales municipales deben ser los que conocen de delitos informáticos, sin realizar ninguna distinción entre las conductas ejecutadas, toda vez que no solamente ellos deberian conocer de este tipo de conductas sino también deberia materializarse una asignación a los jueces

penales del circuito para que ellos también conozcan de este tipo de delitos, complementando dicha designación con la formación en delincunencia informática que deben tener estos profesionales, como la determinación de la cuantía de los procesos que seran objeto de litigio.

2.3. Derecho a la Intimidad.

Resaltando la protección constitucional que tiene este Derecho, es importante precisar que con la ejecución de estas conductas delicitivas, se genera una afectación grave al derecho a la intimidad de las personas, es por tal razón que el tratamiento, reiteramos, de la iformación que sea objeto de estudio en el proceso, y que sea recolectada a lo largo de este, debe contar con todas las garantias y la protección necesaria, para que en el transcurso de su extracción y estudio no pueda sufrir ningun tipo de modificación, ya que los datos que aquí se manipulan, generalemnte pueden sufrir facilmente, algún tipo de daño que impida que puedan ser utilizados y analizados de manera correcta dentro de un caso, afectando de esta manera las garantías constitucionales de las personas afectadas con este tipo de delincuencia informática.

2.4. Derecho a la protección de datos personales.

Este derecho se encuentra ligado al derecho a la intimidad, toda vez que, con la comisión de las conductas delictivas en relación a los delitos informáticos, establecidos en el ordenamiento jurídico de nuestro país, se genera una afectación grave por lo general a aquellos datos que son considerados como sensibles en la legislación colombiana, y frente a los cuales debe existir en el desarrollo del proceso, un tratamiento adecuado y protector, en

aras de no realizar ningún tipo de afectación en primer lugar al derecho a la intimidad de las personas, relacionado con la manipulación de su información y datos personales, como también debe existir un tratamiento limpio y defensor de todas las garantías necesarias para no alterar en ningún aspecto la información que tengan algún tipo de relación con la comisión de delitos informáticos.

CAPÍTULO IV FACTORES GENERADORES DE VULNERACIÓN DE DERECHOS A LAS PERSONAS QUE SUFREN DE CONDUCTAS DELICTIVAS CIBERNÉTICAS

1. Carencia de legislación sobre delitos informáticos

A pesar de la existencia de la ley 1273 del año 2009, en Colombia, y en el mundo los avances en relación a las herramientas informáticas y nuevas tecnologías es constante y por esta razón la actualización de herramientas normativas que permitan la protección de los derechos de las personas que puedan ser vulnerados por la ejecución de la ciberdelincuencia es de vital importancia, actualización, que debe ejecutarse de manera conjunta con el desarrollo de estas nuevas tecnologías, todo esto en aras de proporcionar a personas tanto naturales como jurídicas, las herramientas y medios idóneos para reclamar la protección de los derechos que resulten vulnerados, por tal razón en la actualidad la existencia y aplicabilidad de la ley 1273 de 2009, es insuficiente para abarcar la cantidad de delitos informáticos que se ejecutan diariamente en nuestro país, y que avanzan a la par de las nuevas tecnologías que se desarrollan a nivel global.

1.1. Carencias de legislación orientada al desarrollo procesal de estas conductas.

En concordancia con el punto tratado anteriormente, dentro de la mencionada ley que regula toda la temática relacionada con delitos informáticos, encontramos que los jueces penales municipales, sin importar el delito que se ejecute son los conocedores de este tipo de conductas delictivas, por tal razón, de conformidad con lo desarrollado en este trabajo que se hace necesario el desarrollo de tres instrumentos que permiten un desarrollo procesal adecuado de aquellas conductas que sean investigadas.

Estos instrumentos se basan principalmente en los siguiente:

1. En primer lugar, se hace necesaria la capacitación de todos aquellos profesionales que desarrollen y deban conocer la temática de la ciberdelincuencia, estructurando de esta manera un programa que permita capacitar a Jueces, Defensores Públicos, Fiscales etc., en los temas básicos, relacionados con la delincuencia informática, y los avances que estos delitos presenten.
2. La determinación de la cuantía, dependiendo del caso objeto de estudio, toda vez que la información, y los datos de las personas no deben tener una misma valoración.
3. Por último y reuniendo los dos factores expuestos anteriormente, la asignación del juez penal del circuito para conocer de determinados delitos, toda vez que el juez penal municipal no es el único que debe conocer de estas conductas delictivas.

Lo anterior en aras de proporcionar las garantías procesales adecuadas y efectivas para el manejo y la penalización de los delitos informáticos en el país.

1.2. Factores económicos.

De acuerdo al factor económico que se afecta y el costo del cibercrimen, es importante referenciar los datos proporcionados en el informe: amenazas del Cibercrimen en Colombia 2016-2017, en el cual se destacan los siguientes puntos:

1. La comisión de delitos informáticos genera un costo de alrededor de quinientos setenta y cinco millones de dólares a nivel mundial.

2. En Latinoamérica, se genera un costo de aproximadamente noventa millones de dólares, por la comisión de delitos informáticos

3. Una de las principales afectaciones económicas se construye debido a que las empresas que resultan afectadas por la comisión de este tipo de conductas, no denuncian, toda vez que para ellos esto genera una imagen negativa frente a sus mecanismos de seguridad, lo cual concluye en generar una sensación de desconfianza en sus usuarios o clientes.

4. a nivel nacional se generan perdidas aproximadamente por un valor de un billón de pesos. (Policia Nacional, Centro Cibernético Policial , 2017)

1.3. Costos de un análisis forense de delitos informáticos en Colombia.

En primer lugar, es importante tener en cuenta que el análisis forense, es un sistema informático es una ciencia moderna que permite reconstruir lo que ha sucedido en un sistema tras un incidente de seguridad. Este análisis puede determinar quién, desde dónde, cómo, cuándo, y qué acciones ha llevado a cabo un intruso en los sistemas afectados por un incidente de seguridad (Lopez, 2009).

Por ende, los costos que conllevan la realización de este tipo de análisis forense a un sistema informático afectado por la comisión de algún tipo de conducta delictiva perteneciente al tema de la ciberdelincuencia, son bastante elevados.

Este método, se basa en el uso de herramientas de avanzada tecnología, con la finalidad de garantizar la adecuada protección de los datos que se procesan y se estudian, y adicional a esto, también se hace necesario que los encargados de poner en practica esta disciplina, sean personas con conocimientos especializados en temas informáticos en aras de garantizar un estudio adecuado e idóneo frente a los datos y dispositivos analizados.

Pero la implementación y la utilización de estas herramientas electrónicas y de uso forense, tienen un costo elevado que para el año 2016, el cual se calculaba en un valor aproximado de $180.654.600, para un equipo de análisis forense, el cual no incluye el valor de capacitación del personal que lo utilizaría, pero es importante resaltar que en la mayoría de los casos, el manejo de estos equipos se efectúa por personal de la Policía Nacional, más no por profesionales que trabajen de manera permanente en materia de sistemas, por lo cual el traslado constante de este personal, también es un factor que perjudica la implementación de ésta práctica.

De conformidad con el valor referenciado anteriormente, actualmente el costo de esta disciplina se calcula aproximadamente en $171.041.400, por ende, se evidencia que, aunque se da una disminución de costos, la práctica del análisis forense continua teniendo un valor bastante elevado para su ejecución.

1.4. Conocimiento tecnológico de los jueces penales municipales.

De conformidad con el conocimiento tecnológico y especial con la capacitación que poseen los jueces penales municipales, frente a los delitos informáticos, este tema va ligado con la falta de implementación de herramientas normativas, toda vez, que la sola existencia de la ley 1273 promulgada en el año 2009, no es una herramienta suficiente, teniendo en cuenta el ritmo con el que avanzan las nuevas tecnologías, y de igual forma la ejecución de delitos informáticos, que avanzan de manera conjunta al desarrollo de estos nuevos materiales tecnológicos, es por esta razón, que dentro de nuestra legislación, el conocimiento y capacitación de los jueces frente al cibercrimen, es prácticamente nulo, ya que debería existir un programa que capacite a estos profesionales, especialmente en relación a la valoración de las pruebas digitales presentadas dentro de un proceso.

Toda vez que si no se tiene una referencia y una formación mínima en los aspectos teóricos y técnicos que tengan relación con la ciberdelincuencia, gran parte del material probatorio de carácter digital no se valoraría de manera correcta y de esta manera no se prestarían las garantías procesales idóneas a aquellas personas que se encuentren vinculadas en el proceso, ya que como hemos visto a lo largo del presente documento, este tipo de evidencia, debe contar con un tratamiento especial, tratamiento que debe ser desarrollado por personas especialistas en la materia.

1.5. Investigación de la Fiscalía General de la Nación y unidad de delitos informáticos

En relación al tratamiento dado a los delitos informáticos en nuestro país, una vez presentada la denuncia, e iniciado el respectivo proceso de carácter penal, se da la

asignación de un Fiscal al caso, y de conformidad a esto se empiezan a surtir todas las etapas procesales de este.

Es importante mencionar dos aspectos:

1. Quien brindan apoyo a la Fiscalía General de la Nación en relación con los procesos que involucran delitos informáticos, es el Centro Cibernético Policial de la Policía Nacional.
2. La Fiscalía General de la Nación, cuenta con el manual de procedimientos para cadena de custodia, en el cual se evidencia la notoria falta de implementación de elementos relacionados con el manejo de evidencia de carácter digital, toda vez que este manual se centra en el manejo que se debe tener principalmente con evidencia Física.

CAPITULO V. PROPUESTA DE PROYECTO DE LEY QUE MODIFIQUE LA ASIGNACIÓN DE COMPETENCIAS DE LOS JUECES PENALES MUNICIPALES QUE CONOZCAN DE LAS CONDUCTAS PUNIBLES DESCRITAS POR LA LEY 1273 DE 2009 Y EL TRATAMIENTO PROCESAL EN LA LEY 906 DE 2004

1. Exposición de motivos

La ley 1273 del año 2009, es aquella "por medio de la cual se modifica el Código Penal, y se crea un nuevo bien jurídico tutelado, denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones", por ende, esta reforma busca

modificar el artículo 3° de la mencionada ley bajo los siguientes motivos:

2. Objetivos

- Modificar la asignación de competencia de los jueces penales que deben conocer de la comisión de delitos informáticos, teniendo en cuenta una previa valoración de la información afectada, en aras de asignar la competencia, según la cuantía de estos delitos.

- Crear con esta modificación los mecanismos y elementos adecuados y necesarios para proteger las garantías constitucionales de los ciudadanos afectados por la comisión de delitos informáticos.

3. justificación

En relación con el avance constante de las nuevas tecnologías, y junto con este avance, la evolución de los delitos informáticos, tanto a nivel nacional como mundial, se hace necesario la actualización constante de las herramientas normativas, que regulan la ciberdelincuencia en nuestro país, por tal razón la presente reforma pretende modificar la asignación de competencia de los jueces penales, ya que según lo establecido dentro de la ley 1273 del año 2009, solamente conocen de delitos informáticos los jueces penales municipales, asignación que resulta errada, teniendo en cuenta que la información de las personas no tiene el mismo

valor, ya que en el ámbito social, económico, político y cultural, las personas juegan roles diferentes, y tienen grados de influencia distintos, por tal razón la información que resulte afectada por la comisión de delitos informáticos no debe tener el mismo valor.

Es por este motivo, que al diferenciar en primer lugar la cuantía por la comisión de estas conductas, se debe revisar la asignación de los jueces conocedores del proceso, que no deben ser solamente los jueces penales municipales, sino también los jueces penales del circuito.

4. Contenido

El contenido de la presente reforma, se estructura en dos partes:

1. Modificar el artículo 3° de la ley 1273 de 2009, reestructurando el numeral 6 adicionado al artículo 37 ley 906 de 2004.

2. Adicionar el numeral 4 al artículo 36 de la ley 906 del año 2004.

Por lo anterior, el proyecto de ley quedaría de la siguiente manera:

PROYECTO DE LEY No _____ _____ DE 2018

Por medio de la cual se modifica el artículo el artículo 3° de la ley 1273 del año 2009, y se adicional el numeral 4 al artículo 36 de la ley 906 del 2004.

ARTÍCULO PRIMERO: OBJETO. En aras de garantizar la protección de las garantías fundamentales con las que deben contar los ciudadanos del territorio nacional, al momento de

realizar la asignación de competencia de los jueces penales, frente al estudio de los delitos informáticos que se adelantan en la jurisdicción penal, la asignación se debe realizar teniendo en cuenta una previa valoración de la información afectada, en aras de identificar la cuantía y de esta manera realizar la asignación del proceso al juez idóneo para su conocimiento.

ARTÍCULO SEGUNDO: Artículo 3° de la ley 1273 del año 2009, quedará de la siguiente manera:

Adiciónese al artículo 37 del Código de Procedimiento Penal con la modificación al numeral 6 así:

6. De los delitos contenidos en el título VII Bis, en cuantía equivalente a una cantidad no superior en pesos de ciento cincuenta (150) salarios mínimos mensuales legales vigentes al momento de la comisión del hecho.

ARTÍCULO TERCERO. Adiciónese al artículo 36 del Código de Procedimiento el numeral 4 así

4. De los delitos contenidos en el título VII Bis, en cuantías superiores en pesos a ciento cincuenta (150) salarios mínimos mensuales legales vigentes al momento de la comisión del hecho, conocerán los jueces penales del circuito.

ARTÍCULO CUARTO: VIGENCIA Y DEROGATORIAS. La presente ley rige a partir de su promulgación y deroga las normas que le sean contrarias.

CONCLUSIONES

1. Es necesario entender que debido a los grandes avances que se han originado en los diversos campos tecnológicos a nivel mundial, y la necesidad que constituye hoy en día el uso de estas nuevas tecnologías en la cotidianidad de la mayoría de los habitantes del mundo, ha ido tomando fuerza y desarrollándose a gran escala la ejecución de una diversidad de delitos informáticos que atacan diariamente diferentes sectores de nuestra sociedad, generando con esta ejecución, daños que en diversos casos resultan irreversibles y que dejan como resultado gran afectación no solo en los sistemas informáticos, sino también en la vulneración y daño que generan en la información y datos personales de aquellos que resultan afectados.

Es por esta razón, que la actualización de las herramientas normativas dentro del ámbito legislativo de los diversos países debe ser concordante con la realidad que estamos atravesando en este momento, situación frente a la cual, la legislación colombiana aún se encuentra atrasada en la implementación de aquellos elementos normativos que regulen de manera adecuada la comisión de estos delitos y que, con esta regulación, proteja de manera eficiente las garantías constitucionales de todos los habitantes del territorio nacional.

Es así como observamos que en relación a este tema, solamente poseemos la ley 1273 promulgada en el año 2009, fecha desde la cual, a la actualidad se ha generado un sin número de adelantos tecnológicos y con ellos, una evolución de la delincuencia informática; dentro de esta ley encontramos tipificados una serie de delitos, que en la actualidad no resultan suficientes de conformidad con la cantidad de ataques que

anualmente se ejecutan en nuestro país, y con la cantidad de nuevas herramientas utilizadas para esta comisión, un ejemplo de esto lo encontramos en la implementación de las monedas electrónicas como Bitcoin a modo de medio para la comisión de diversas conductas delictivas.

Razón por la cual, es una necesidad, modificar o implementar una nueva normatividad, que regule todas aquellas situaciones relacionadas con la ciberdelincuencia que han generado un avance y una evolución a lo largo de los años, normatividad que debe poseer un estudio y actualización constante, la cual permita tener un referente moderno, de aquellos ataques informáticos que se ejecutan, y que afectan a particulares, entidades empresariales y entes gubernamentales en un número bastante alto y con un crecimiento elevado y constante a lo largo de los años en nuestro país.

2. En concordancia con el punto anterior, y en relación a la falta de actualización de la legislación colombiana en materia de delitos informáticos, vemos como es evidente también la falta de formación y capacitación de aquellos profesionales del Derecho, encargados de conocer y llevar a su culminación aquellos procesos relacionados con la delincuencia informática.

Razón por la cual todos los jueces, Fiscales, Defensores Públicos y demás funcionarios encargados de conocer de este tipo de casos, deben contar con una actualización constante en esta materia, y también poseer algún tipo de formación relativa a temas tanto teóricos como técnicos, referentes a los delitos informáticos, formación, que se hace necesaria, ya que en muchos de los procesos que se adelantan, al no poseer los conocimientos básicos en delincuencia informática muchas veces la valoración de aquellos elementos probatorios no

va a ser la adecuada, o simplemente no se realizará esta valoración, afectando de manera grave los derechos de las personas que resulten afectadas y se vean involucradas en un proceso de este tipo.

Encontrándose por tal razón necesario, de manera conexa a la actualización de nuestra normatividad, la implementación de programas y planes de capacitación de todos los funcionarios que deban relacionarse y conocer este tipo de delitos. Formación que debe realizarse por personal experto y conocedor de los temas relacionados con la ciberdelincuencia y de esta manera garantizar un desarrollo apropiado de los procesos en la jurisdicción penal.

3. Por otro lado, se debe tener presente, que la mayor afectación que se genera con la comisión de estas conductas delictivas, es a la información y datos personales de las víctimas; y este es un punto que resulta importante mencionar toda vez que, en nuestra legislación, a modo de ejemplo el hurto de información a un estudiante universitario, y el hurto de información a una entidad bancaria de gran reconocimiento, tienen el mismo valor, y por ende todos estos delitos deben ser conocidos por los jueces penales municipales.

Ésta es una situación que es completamente errónea, teniendo en cuenta que la información que posea un estudiante universitario, no debe tener igual valor que la información hurtada a una entidad bancaria de gran reconocimiento, es por tal razón que teniendo claros estos casos expuestos a modo de ejemplo, se hace necesaria, dar una valoración adecuada a la información y datos que puedan resultar afectados por la comisión de algún delito informático, evaluando diversos factores, y no simplemente, establecer que la información

de todos tiene el mismo valor, y de esta manera realizar un asignación correcta de competencia en la jurisdicción penal para el conocimiento de estos procesos.

4. Por último y reuniendo todos los puntos expuestos con anterioridad, se hace necesaria, una modificación y actualización a nuestra legislación, en el tema referente a la asignación de competencia de los jueces penales que deben conocer de aquellos procesos que involucren la comisión de delitos informáticos.

Modificación que se debe realizar con la inclusión de los jueces penales del circuito como conocedores de aquellos procesos que, por razón de cuantía, previo análisis valorativo de la información o datos afectados, no puedan conocer los jueces penales municipales.

Todo esto con la finalidad, de implementar un sistema normativo actualizado en materia de ciberdelincuencia, y de esta manera garantizar que el funcionario encargado de dirimir el conflicto sea la persona idónea y capacitada para culminar de manera adecuada un proceso de delincuencia informática.

REFERENCIAS

ley 1273 de 2009. (2009). Recuperado el 2018, de http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Ascanio, M. B. (s.f.). *Los papeles de Panamá y sus implicaciones periodísticas y sociales* . Recuperado el 11 de marzo de 2018, de http://gumilla.org/biblioteca/bases/biblo/texto/COM2016174_61-71.pdf

Macedo, V. R., & Rosales, M. S. (2017). *WannaCry: Análisis del movimiento de recursos financieros en el blockchain de bitcoin.* Recuperado el 11 de marzo de 2018, de http://www.rcs.cic.ipn.mx/rcs/2017_137/WannaCry_%20Analisis%20del%20movimiento%20de%20recursos%20financieros%20en%20el%20blockchain%20de%20bitcoin.pdf

Policia Nacional, Centro Cibernético Policial . (2017). *Amenazas del Cibercrimen en Colombia 2016-2017.* Policia Nacional , Centro cibernético Policial.

Parlamento Erupeo y del Consejo. (2002). *Directiva 2002/58/CE relativa al tratamiento de los datos personales y la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).* Recuperado el 19 de marzo de 2018, de https://edps.europa.eu/sites/edp/files/publication/dir_2002_58_es.pdf

Consejo de la Unión Europea. (24 de febrero de 2005). *Decisión Marco 2005/222/JAI del Consejo de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información.* Recuperado el 18 de marzo de 2018, de https://www.boe.es/doue/2005/069/L00067-00071.pdf

Bosch, M. F. (2015). *El Asilo Político: El caso Assange.* Recuperado el 18 de Marzo de 2018, de http://www.recercat.cat/bitstream/handle/2072/257370/TFG-FORN-2015.pdf?sequence=1

Sentencia SP 1245-2015 (11 de febrero de 2015).

Sentencia T-550/12, T-3387538 (Corte Constitucinal 13 de Julio de 2012).

Sentencia T-260/12 (Corte Constitucional 2012).

Sentencia C-334 de 2010 (Corte Constitucional 12 de mayo de 2010).

Sentencia T 308 de 2014 (2014).

Ley 906 de 2004 Por la cual se expide el Código de Procedimiento Penal. (s.f.). Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_0906_2004.html

Rogriguez, J. M. (2011). *Metodos de investigación cualitativa* . Recuperado el 22 de marzo de 2018, de http://www.cide.edu.co/doc/investigacion/3.%20metodos%20de%20investigacion.pdf

Bolaño, I. M., & Tarriba , F. J. (2012). *Caracterización de los delitos informáticos en Colombia.* Recuperado el 19 de marzo de 2018, de http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewFile/126/149

Convenio sobre la Ciberdelincuencia Budapest, 23.XI.2001. (s.f.). Obtenido de http://www.cienciaspenales.net/files/2016/10/1.-CONVENIO-DEL-CONSEJO-DE-EUROPA-SOBRE-CIBERDELINCUENCIA.pdf

Resolución del Consejo No 2002/ C43. (28 de Enero de 2002).

Gomez, A. D. (2011). *El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El convenio de Budapest.*

Recuperado el 19 de marzo de 2018, de https://dialnet.unirioja.es/servlet/articulo?codigo=3732276

Garavilla, M. E. (s.f.). *Delitos informáticos.* Recuperado el 19 de Marzo de 2018, de https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080526_32.pdf

J. G. (2010). *Panorama del derecho informático en América Latina y el Caribe*. Recuperado el 19 de marzo de 2018, de https://repositorio.cepal.org/bitstream/handle/11362/3744/1/S2009865_es.pdf

González, J. A. (2013). *Delitos Informáticos: Su clasificación y una visión general de las medidas de acción para combatirlo.* Recuperado el 2018, de http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf

Vieites, A. G. (s.f.). *La lucha contra el ciberterrorismo y los ataques informáticos.* Recuperado el 19 de marzo de 2018, de http://www.edisa.com/wp-content/uploads/2014/08/La_lucha_contra_el_ciberterrorismo_y_los_ataques_informaticos.pdf

S. M. (12 de marzo de 2017). ciberterrorismo .

O. M. (2012). *Ciberterrorismo.* Recuperado el 19 de marzo de 2018, de http://www.egov.ufsc.br/portal/conteudo/ciberterrorismo

Martinez, N. R. (08 de agosto de 2016). *La amenaza cibernética: ciberguerra y ciberdefensa.* Recuperado el 2018, de https://cisde.es/observatorio/la-amenaza-cibernetica-ciberguerra-y-ciberdefensa

Martín, R. M. (s.f.). *Deontología y legislación informática.* Obtenido de https://previa.uclm.es/profesorado/raulmmartin/Legislacion/apuntes.pdf

Martínez, M. G. (2015). *Conceptos básicos de derecho informático.* Recuperado el marzo de 2018

Pino, S. A. (2008). *Delitos informáticos: Generalidades.* Recuperado el 22 de marzo de 2018

Magariños, F. R. (s.f.). *Nuevos delitos informáticos Phising, Pharming, Hacking y Cracking.* Recuperado el 19 de marzo de 2018

Valdes, J. T. (1991). *Derecho informático.* México: Universidad Nacional autónoma de México.

N. W. (1980). *Cibernética y sociedad.* México.

Quintero, K. R., & Martin, E. L. (s.f.). *"EL PHISING, PHARMING Y SPOOFING".* Obtenido de http://www.eduardolagaron.com/wp-content/uploads/2011/02/phising-pharming-y-spoofing2.pdf

Gomez, M. M. (2001). *El sabotaje informático: entre los delitos de daños y desordenes públicos* .

Criado, M. P., & Barrego, B. T. (2016). *Redes sociales y ciberterrorismo. Las TIC como herramienta terrosrista.* . Obtenido de http://www.redalyc.org/pdf/310/31048481030.pdf

G. S. (s.f.). *¿Qué es la ciberguerra?* Obtenido de http://www.pensamientopenal.com.ar/system/files/2016/02/doctrina42952.pdf

Alvarez, V. M., & Cocheiro, R. A. (s.f.). *Virus Informáticos.* Obtenido de http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/08%20-%20Virus%20Informaticos.pdf

Facua . (s.f.). *el SPAM que es y como enfrentarte a el* . Obtenido de https://www.facua.org/es/guias/guia141.pdf

Quezada, M. P. (s.f.). *REDES SOCIALES Y CIBERBULLYING TEMA EMERGENTE EN LA INVESTIGACIÓN EDUCATIVA.* Obtenido de http://inie.ucr.ac.cr/tercer-congreso/memoria/documentos/12/redessocialesyciberbullyingtemaemergente.pdf

INTECO. (s.f.). *GUIA GESTIÓN DE FUGA DE INFORMACIÓN.* Obtenido de https://www.incibe.es/extfrontinteco/img/File/intecocert/Formacion/EstudiosInformes/guia_gestion_fuga_informacion.pdf

Azamar, B. L. (s.f.). *Software malintencionado e infeccioso.* Obtenido de http://www.unpa.edu.mx/~blopez/Computacion/complementario/VirusYotrosMalware.pdf

A. C. (s.f.). *Edward Snowden: ¿Traidor o héroe?* Obtenido de http://ethicsunwrapped.utexas.edu/wp-content/uploads/2017/03/38-Edward-Snowden-¿Traidor-o-héroe.pdf

Sentencia T 040 de 2013, T-3.623.589 (Corte Constitucional 28 de enero de 2013).